PRIVACY IN THE HANDS OF THE GOVERNMENT: THE PRIVACY OFFICER FOR THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCIAL AND ADMINISTRATIVE LAW

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

FEBRUARY 10, 2004

Serial No. 85

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

91–751 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

CHRIS CANNON, Utah *Chairman*

HOWARD COBLE, North Carolina
JEFF FLAKE, Arizona
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
STEVE CHABOT, Ohio
TOM FEENEY, Florida

MELVIN L. WATT, North Carolina
JERROLD NADLER, New York
TAMMY BALDWIN, Wisconsin
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

RAYMOND V. SMIETANKA, *Chief Counsel*
SUSAN A. JENSEN, *Counsel*
DIANE K. TAYLOR, *Counsel*
JAMES DALEY, *Full Committee Counsel*
STEPHANIE MOORE, *Minority Counsel*

CONTENTS

FEBRUARY 10, 2004

OPENING STATEMENT

WITNESSES

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PRIVACY IN THE HANDS OF THE GOVERNMENT: THE PRIVACY OFFICER FOR THE DEPARTMENT OF HOMELAND SECURITY

TUESDAY, FEBRUARY 10, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCIAL
AND ADMINISTRATIVE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3:02 p.m., in Room 2141, Rayburn House Office Building, Hon. Chris Cannon (Chair of the Subcommittee) presiding.

Mr. CANNON. Thank you all for coming out.

Let me begin by hereby welcoming our esteemed witnesses, some of whom I've had the pleasure of working with on privacy issues and other matters over the years.

I also want to note that immediately following the hearing we have scheduled a markup of H.R. 338, the "Defense of Privacy Act." Indeed, if we have a critical mass of Members to report that bill, we may recess this hearing briefly to accomplish that task.

The title of today's hearing, Privacy in the Hands of Government: The Privacy Officer for the Department of Homeland Security, clearly sets out what we plan to examine this afternoon. We will review the work and responsibility of the Department's Privacy Officer and consider whether the statute creating this position sufficiently addresses concerns about the Department's handling of personally identifiable information.

We will also examine how the Department has met the rather daunting challenge of detecting and deterring terrorism while safeguarding Americans from unwanted or unwarranted Governmental intrusion. I suppose all intrusion is unwanted. A lot of it is, in fact, unwarranted.

For those of you don't know, the creation of the Privacy Officer Position in the Department of Homeland Security marked the first time that Congress statutorily mandated a Federal agency to appoint a senior official to be primarily responsible for privacy policy and compliance matters. Indeed, this Subcommittee, with the support of our Chairman, Jim Sensenbrenner, played a major role in ensuring that the legislation establishing the Department of Homeland Security not only mandated the appointment of a Privacy Officer, but specified the officer's responsibilities. This was done in response to concerns expressed on a bipartisan basis about the antici-

pated agency's ability to collect, manage, share, and secure personally identifiable information.

One of the principal statutory responsibilities of the DHS Privacy Officer, as set out by statute, is the duty to assure—to assure that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of personal information.

In addition, the Privacy Officer must assure that personal information is handled in full compliance with the Privacy Act and assess the effect on privacy of the Department's proposed rules. These are two of the areas that we hope to focus on during the course of today's hearing.

Pursuant to this legislation, Department of Homeland Security Tom Ridge last April appointed Nuala O'Connor Kelly to serve as the Department's Privacy Officer. Since her appointment, Ms. O'Connor Kelly has played an active role in various terrorist detective initiatives undertaken by DHS. One of those projects has been the Computer-Assisted Passenger Prescreening System, also known as CAPPS II, which is intended to improve airline security.

In addition, Ms. O'Connor Kelly prepared a privacy impact assessment for the United States Visitor and Immigration Status Indicator Technology Program, also known as the US-VISIT program. This program consists of an integrated entry and exit data system designed to record the entry into and exit out of the United States by noncitizens. Last month, US-VISIT entry procedures became operational at 115 airports and 14 seaports together with a pilot test of biometric identification procedures at one airport and one seaport

I should note that today's hearing is one in a series the Subcommittee will hold on the issue of privacy in the hands of Government.

I now turn to my colleague, Mr. Watt, the distinguished Ranking Member of the Subcommittee and ask him if he has any opening remarks?

Mr. WATT. Thank you, Mr. Chairman.

Mr. CANNON. The gentleman is recognized for 5 minutes.

Mr. WATT. Thank you, Mr. Chairman, for convening this hearing today. It must be my day to deal with privacy and identity theft issues. I'll tell you what has transpired today.

I was seated in a meeting with representatives from various Government agencies, one of which was Social Security. And one of their complaints was that Government work is being contracted out to private companies who don't have the kind of responsibility for overseeing privacy and preventing identity left. That meeting lasted for about 20, 30 minutes. During that meeting three things happened.

One, I got placed on my desk the comments for this meeting here this afternoon, which I haven't had a chance to review very thoroughly but I'm going to take a stab at them when I get back to the formal part of this presentation.

Second, I got placed on my desk a message from a newspaper reporter at the Charlotte Observer—which is in my Congressional district in Charlotte, North Carolina—with an attached article which says a Charlotte temporary employment agency left more

than 20 boxes filled with hundreds of job applications on the curbside for the better part of a day Sunday and Monday. And goes on to ask me if I have any comments to make about that.

Then I got placed on my desk, during that same meeting, a letter from our minority leader asking me to join in a letter to the president expressing concerns about the way the CAPPS II program is being—playing itself out and asking the Administration to pay more attention to the dissemination of personal information.

This is a multidimensional problem, not only Government information that we are gathering but private information. We've tried to attack it in various compartmentalized ways through Fair Credit Reporting Act in the Financial Services Committee on which I sit, through various things in this Judiciary Committee, but this is—this already difficult issue has been complicated by the events of September 11. And since then our country has been confronted with the dual aspiration of ensuring the security of our homeland and at the same time preserving and securing the Civil Rights and liberties that make our homeland free and unique.

The creation of the Department of Homeland Security was historic. Homeland Security Act of 2002 created an agency with the primary responsibility of preventing terrorist attacks in the United States, reducing our vulnerability to such attacks, minimizing damage due to any attack, and assisting in our ability to recover from those attacks.

My concern here today however is that the Department not be so vigilant in its terrorist prevention and terrorist detection duties that it undermines our individual freedoms.

Just last May the GAO described the Department of Homeland Security's responsibilities to include "the coordination and sharing of information related to threats of domestic terrorism within the Department and with and between other Federal agencies, State and local governments, the private sector, and other entities".

The report recognized that to accomplish this mission the Department of Homeland Security must access, receive and analyze law enforcement information, intelligence information, and other threat incident and vulnerability information from Federal and non-Federal sources.

Recent newspaper reports indicate that questionable information sharing occurred between JetBlue and Northwest Airlines and law enforcement in order to implement the CAPPS II Computer-Assisted Passenger Prescreening System designed to prescreen airline passengers. Despite the existence of a Privacy Officer within the Department of Homeland Security, the JetBlue and Northwest Airline collaboration with the Government raises serious privacy issues because although these private entities may have their own privacy policies they are not subject to the constraints of the Privacy Act.

This circumstance may lead to a gaping hole in safeguarding the improper dissemination of personal information. This is a hole that I personally tried to plug last year during the Judiciary Committee's consideration of H.R. 4598, the Homeland Security Information Sharing Act. That bill, which did pass the House and has not passed the Senate, would have authorized Federal, State and local entities, including private actors, to share information to the fullest

extent possible in the interest of national security. During its consideration I offered an amendment to the bill that would have placed constraints on the dissemination of personal information which would have prohibited any unauthorized use and that amendment passed in this Committee.

As we listen to the testimony today, I am interested in determining whether it would be useful to resurrect at least the spirit of H.R. 4598 by ensuring that American citizens and those traveling within our borders are fully aware of how their personal information will be collected, used, and disseminated by whatever source in the name of national security.

And that, coincidentally, is exactly what the letter from our minority leadership is encouraging the president to focus his attention on and I'm sure that new Privacy Officer will be—it will filter to you at some point.

So we are delighted to have you here and I appreciate the Chairman calling this hearing. He's known for getting on top of these things when they are topical and interesting and covering many fronts and being in front of the curve, not only reactive but being proactive.

So I appreciate the Chairman getting this convened today, look forward to the witnesses' testimony and to the markup.

Mr. CANNON. I thank the gentleman for those kind comments and I appreciate his bipartisan support. These are important issues that we need to actually move on.

Without objection, the gentleman's entire statement will be placed in the record.

Also, without objection, all Members may place their statements in the record at this point. Any objection?

Hearing none, so ordered.

Without objection, the Chair will be authorized to declare recesses of the Subcommittee today at any point.

Hearing none, so ordered.

I also ask unanimous consent that Members have five legislative days to submit written statements for inclusion in today's hearing record. So ordered.

Are there further opening statements? Mr. Coble?

Mr. COBLE. No opening statement, Mr. Chairman.

Mr. CANNON. Thank you.

I'm pleased to introduce the witnesses for today's hearing. Our first witness is Nuala O'Connor Kelly, the Chief Privacy Officer of the Department of Homeland Security. Ms. O'Connor Kelly was appointed to her current position on April 16, 2003. Just prior to her appointment she served as the Chief Privacy Officer at the Commerce Department.

Before entering public service, Ms. O'Connor Kelly was the Vice President for Data Protection and Chief Privacy Officer for Doubleclick, an online media services company, that she rescued with her privacy policies. I add that as a personal note. In that capacity, Ms. O'Connor Kelly established that company's first data protection department and was responsible for instituting privacy protection policies and procedures for Doubleclick, its clients and partners.

Ms. O'Connor Kelly received her undergraduate degree from Princeton University and masters degree in education from Harvard University and a law degree from Georgetown University Law Center.

Our second witness is the Honorable James Gilmore, the former Governor of the Commonwealth of Virginia. Governor Gilmore, as you will recall, has previously shared with this Subcommittee his vast expertise on technology and Internet policy matters for which we are deeply grateful.

Today Governor Gilmore appears on behalf of USA Secure Corporation, a nonpartisan, not-for-profit think tank which he founded. USA Secure is comprised of technology and infrastructure companies that are affected by and participate in homeland security. It provides a forum for its members to develop integrated solutions regarding homeland security issues.

Of particular relevance to today's hearing is Governor Gilmore's service as the Chairman of the Congressional Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction, all also known as the Gilmore Commission. The Commission was established by Congress to assess Federal, State and local Government's capabilities to respond to the consequences of a terrorist attack. The Gilmore Commission, which recently submitted its final report to the President and Congress, was influential in developing the Department of Homeland Security.

Governor Gilmore received his undergraduate degree in foreign affairs from the University of Virginia and, after a 3-year tour as a U.S. Army counterintelligence agent in West Germany, obtained his law degree at the University of Virginia Law School.

He continues to demonstrate his dedication to homeland security and technology issues as a partner of the law firm of Kelley, Drye, Warren here in Washington, D.C.

Our next witness is Professor Sally Katzen of the University of Michigan Law School. We understand the Professor Katzen appears today solely in her personal capacity and not on behalf of the University of Michigan or any other entity.

Prior to joining academia in 2001, Professor Katzen was responsible for developing privacy policy for the Clinton administration for nearly a decade. As the Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget, she was effectively the chief information policy official for the Federal Government. Her responsibilities included developing the Federal privacy policies, including implementation of the 1974 Privacy Act.

Professor Katzen later served as Deputy Assistant to the President for Economic Policy and Deputy Director of the National Economic Counsel in the White House. Thereafter she became the Deputy Director for Management at OMB.

Before embarking on her public service career, Professor Katzen was a partner in the Washington, D.C. law firm of Wilmer, Cutler and Pickering, where she specialized in regulatory and legislative matters.

Professor Katzen graduated magna cum laude from Smith College and magna cum laude from the University of Michigan Law

School where she was editor-in-chief of the Law Review. Following graduation from law school, she clerked for Judge J. Skelly Wright of the United States Court of Appeals for the District of Columbia Circuit

Our final witness is Jim Dempsey, a Judiciary Committee alum who we are pleased to welcome back. Mr. Dempsey is currently the Executive Director of the Center for Democracy and Technology where he specializes in privacy and electronic surveillance issues.

Before joining the Center, Mr. Dempsey was the Deputy Director of the Center for National Security Studies and also served as Special Counsel to the National Security Archive, a non-governmental organization that uses the Freedom of Information Act to gain the declassification of documents pertaining U.S. foreign policy.

From 1985 to 1994 Mr. Dempsey was Assistant Counsel to the House Judiciary Committee on Civil and Constitutional Rights. Mr. Dempsey obtained his undergraduate degree from Yale College and his law degree from Harvard Law School.

We have a very distinguished panel. I extend to each of you my warm regards and appreciation for your willingness to participate in today's hearing.

In light of the fact that your written statements will be included in hearing record, I request that you limit your oral remarks to 5 minutes. Accordingly, please feel free to summarize and highlight the salient points of your testimony. And you have a light on—I think you're all familiar with this lighting system. It goes yellow when you have a minute left. When it goes red you don't have to stop, but we'd appreciate it if you'd sort of wrap up, if you could, so that Members have the opportunity of asking questions.

After all the witnesses have presented their remarks, the Subcommittee Members, in the order that they arrive, will be permitted to ask questions of the witnesses subject also to the 5 minute limit.

Ms. O'Connor Kelly, would you now proceed with your testimony?

STATEMENT OF NUALA O'CONNOR KELLY, CHIEF PRIVACY OFFICER, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Ms. O'CONNOR KELLY. Thank you, Mr. Chairman.

Chairman Cannon, Congressman Watt, and Members of the Subcommittee, it is my distinct honor to testify before you today on the activities of the United States Department of Homeland Security's Privacy Office, which I am privileged——

Mr. CANNON. Ms. O'Connor Kelly, if you wouldn't mind, we will restart your clock, but I think we have a reporting quorum. So consistent with our earlier orders, we are going to recess this hearing for a period and try and report out this bill. So we will go at this moment to our markup.

Do any of you have—I don't think this is going to take a long period of time. Do any of you have significant other obligations that we need to meet?

Thank you. If you don't mind then, we will be recessed from the hearing and we will open our markup.

[Whereupon, at 3:20 p.m., the hearing was recessed, to reconvene this same day at 3:35 p.m.]

Mr. CANNON. And now, Ms. O'Connor Kelly, we appreciate your indulgence and the indulgence of the panel.

I would now like to be informed about what is going on in the new world of privacy. Thank you.

If you would like to proceed, we will reset the clock.

Ms. O'CONNOR KELLY. Thank you, Mr. Chairman, and thank you Congressman Watt and all the Members of the Committee.

It is a great pleasure and an honor to be with you today to talk about the Department of Homeland Security's Privacy Office, which I am privileged to lead as the Department's first Privacy Officer.

The creation of the Department of Homeland Security and its many programs raise no shortage of important privacy and civil liberty issues for this Nation to address. The Department, led by Secretary Ridge, and this Administration, led by President Bush, are committed to addressing these critical issues as we seek to strengthen our homeland. A crucial part of this commitment is the mission of the Privacy Office at the Department of Homeland Security.

Before this office officially opened its doors, Secretary Ridge articulated his vision for our office, stating that the Privacy Office will be involved from the very beginning with every policy initiative and every program initiative that we consider, to ensure that our strategy and our actions are consistent with not only the Federal privacy safeguards already on the books but also with the individual rights and civil liberties protected by our laws and our Constitution.

As Members of this Subcommittee are uniquely aware, the enabling statute for the Department of Homeland Security directs the Secretary to appoint a senior official in the Department to assume primary responsibility for privacy policy. That legislation reflects, I believe, a growing sensitivity and awareness on the part of our citizens regarding personal data flows in the public and in the private sector and the particular concerns surrounding this melding of 22 former separate agencies along with the unique mission and data collection activities that each of those agencies brings.

The DHS Privacy Office works to promote best practices with respect to privacy and to infuse fair information principles and practices into the DHS culture. A major goal for my tenure as Chief Privacy Officer is to operationalized privacy throughout the Department. We are doing this not only by working with Secretary Ridge and our senior policy leadership of the various agencies and directorates across the Department but also with our Privacy Act and Freedom of Information Act teams, as well as the operational, policy, and program staff throughout the Department.

Through internal educational outreach and the establishment of internal clearance procedures and milestones for program development we are helping this Department consider privacy whenever developing new programs or revising existing ones. We are evaluating the use of new technologies to ensure that privacy protections are considered in the development and implementation of these programs at each stage.

In this process Departmental professionals have become educated about the need to consider and the framework for considering that privacy impact of technology decisions. We are reviewing Privacy Act systems notices before they are sent forward and ensuring that we collect only those records that are necessary to support the Department's mission.

We also guide Departmental agencies in developing appropriate privacy policies for their programs and serve as a resource for any questions that arise concerning privacy, information collection, or disclosure.

And the Privacy Office, of course, works closely with various Departmental policy teams, the Office of General Counsel, the Chief Information Officers to ensure that the mission of the Privacy Office is reflected in all DHS initiatives.

The Privacy Office also seeks to anticipate and to satisfy public needs and expectations by providing a crucial link between those outside the Department who are concerned about the privacy impact of the Department's initiatives and those inside the Department who are diligently working to achieve the Department's mission.

Our role is not only to inform, to educate, and to lead privacy practice within the Department but also to serve as a receptive audience to those outside the Department who have questions or concerns about the Department's operations. To that end, the Privacy Office has engaged in consistent and substantial outreach efforts to members of the advocacy community, industry representatives, other U.S. agencies, foreign governments, and most importantly, the American public. Our Government and our agency are grounded on principles of openness and accountability tempered, of course, by the need to preserve the confidentiality of the most sensitive personal commercial and Governmental information.

Our work at the Department Privacy Office is proving that it is, in fact, possible to achieve both responsible privacy practices and the critical mission of the Department of Homeland Security.

Issues of privacy and civil liberties are most successfully navigated when the necessary legal, policy, and technological protections are built into the systems or programs from the very beginning. I am often asked whether I view my job as a privacy advocate as at odds with the mission of the Department. And the answer is, without hesitation, no. As Secretary Ridge has articulated on many occasions, the Department of Homeland Security's mission is more than just counterterrorism and more than just the protection of people and places and things. It is the protection of our liberties and our way of life.

That way of life includes the ability to engage in public life with dignity, autonomy, and a general expectation for respect for personal privacy. Thus, the protection of privacy is neither an adjunct nor the antithesis of the mission of the Department of Homeland Security. Privacy protection is, in fact, at the core of that mission.

I thank you for your time and the opportunity to testify before this important Committee and I look forward to hearing my colleagues' testimony and to answering your questions.

Thank you.

[The prepared statement of Ms. O'Connor Kelly follows:]

PREPARED STATEMENT OF NUALA O'CONNOR KELLY

Chairman Cannon, Ranking Member Watt, Members of the subcommittee, and distinguished colleagues on this panel, it is an honor to testify before you today on the activities of the United States Department of Homeland Security's Privacy Office, which I am privileged to lead as the first Chief Privacy Officer of the Department of Homeland Security.

The protection of privacy, of the dignity of the individual, is not a value that can be added on to this or any other organization later, and that is why I am so pleased to have been here from almost the very beginning. This value is one that must be embedded in the very culture and structure of the organization. I know that we can and will succeed in this—not only because our leadership believes in protecting the sanctity of the individual, but also because our over 180,000 employees are also great Americans, who believe in and act on these values—for themselves, their neighbors, and their children—each day.

ESTABLISHMENT OF THE DHS PRIVACY OFFICE

The creation of the Department of Homeland Security and its many programs raise no shortage of important privacy and civil liberties issues for this nation to address. This Department, led by Secretary Tom Ridge, and this Administration, led by President Bush, are committed to addressing these critical issues as they seek to strengthen our homeland. A crucial part of this commitment is support for the creation and the mission of the Privacy Office at the Department of Homeland Security. Secretary Ridge articulated his vision for this office, stating that the privacy office "will be involved from the very beginning with every policy initiative and every program initiative that we consider," to ensure that our strategy and our actions are consistent with not only the federal privacy safeguards already on the books, but also "with the individual rights and civil liberties protected by our laws and our Constitution."

As Members of this subcommittee are uniquely aware, the enabling statute for the Department of Homeland Security contains Section 222, which directs the Secretary to appoint a senior official in the Department to assume primary responsibility for privacy policy. This includes conducting and oversight of formal Privacy Impact Assessments to "assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information." This office also oversees the Department's compliance with the Privacy Act of 1974 and the Privacy Impact Assessment requirements of the Electronic Government Act of 2002, and is directed to "evaluate legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government." Uniquely and importantly, under the enabling statute, the DHS Chief Privacy Officer provides an annual report to Congress on the activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act, internal controls, and other matters.

KEY LEGAL FRAMEWORKS ENFORCED BY THE PRIVACY OFFICE

One of the primary legal frameworks underlying the mission of the DHS Privacy Office is, obviously, the federal Privacy Act of 1974. The Privacy Act, 5 U.S.C. § 552a, provides a code of fair information practices that governs the collection, maintenance, use, and dissemination of personal information by federal agencies. Emanating from concerns about the ability to aggregate personal information—partly due to new technologies like mainframe computers of that day—this law provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by some part of the executive branch of the federal government. The law provides robust advance notice, through detailed "system of records" notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records. The Privacy Act is our country's articulation of Fair Information Principles; the Act both protects the information of our citizens and also provides our citizens rights to access that data.

Under the Freedom of Information Act, 5 U.S.C. § 552, the principle that persons have a fundamental right to know what their government is doing is enforced on a daily basis. Almost any person at any time has the right to query a federal agency for documents and records. Our government and our agency are grounded on principles of openness and accountability, tempered, of course, by the need to preserve the confidentiality of sensitive personal, commercial, and governmental information.

The Freedom of Information Act is the primary statute that attempts to balance these countervailing public concerns. A robust FOIA/PA program is a critical part of any agency's fundamental processes; it helps to provide assurance to the public that, in pursuing its mission, an agency will also pursue balanced policies of transparency and accountability while preserving personal privacy. The U.S. federal government will spend hundreds of millions of dollars processing and responding to FOIA requests next year, and thousands of federal workers will spend all or part of their day compiling responses to those requests. Our agency alone has over 300 staff members across the Department who work full or part-time on Privacy Act and FOIA issues.

This past fall, the Office of Management and Budget released its guidance under Section 208 of the E-Government Act of 2002—which mandates Privacy Impact Assessments for all federal agencies when there are new collections of, or new technologies applied to, personally identifiable information. This, really a third pillar of the privacy framework at the federal level reflects, once again, a growing reliance on technology to move data—both in government spaces and on the Internet. With the addition of the privacy provisions of the E-Government Act to existing privacy protections, our citizens now benefit from a comprehensive framework within which government considers privacy in the ordinary course of business. The Act and underlying guidance synthesize numerous prior statements and guidance on privacy practices and notices, and will assist privacy practitioners in prioritizing their efforts. In particular, the guidance provides direction on the content of privacy policies and on the machine-readability of privacy policies.

Further, the act outlines the parameters for privacy impact assessments. Although in use by some agencies already, generally privacy impact assessments are a new and important tool in the toolbelt of privacy practitioners across the federal government. These new requirements formalize an important principle: that data collection by the government should be scrutinized for its impact on the individual and that individual's data . . . and ideally before that data collection is ever implemented. The process, the very exercise of such scrutiny, is a crucial step towards narrowly tailoring and focusing data collection towards the core missions of government. This practice should provide even greater awareness, both by those seeking to collect the data and those whose data is collected, of the impact on the individual and the purpose of the collection.

I am pleased to have been a small part of the discussions towards the development of guidance on privacy impact assessments. These new requirements set the bar high for privacy practitioners. These requirements also reflect, I believe, a growing sensitivity and awareness on the part of our citizens regarding personal data flows in the public and private sectors. I believe that this guidance will allow federal agencies to respond to citizens' concerns about these activities and also to be current with, or perhaps even slightly ahead of, the evolution of privacy practices in the private sector.

Under the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them. A robust FOIA/PA program is imperative to provide the public with assurances that any information DHS collects is being maintained consistent with all legal and regulatory requirements.

OPERATIONALIZING PRIVACY THROUGHOUT THE DEPARTMENT OF HOMELAND SECURITY

Best Practices through Management Leadership

The DHS Privacy Office works to promote best practices with respect to privacy and infuse respectful information privacy principles and practices for all employees into the DHS culture. A major and substantial goal at the outset for my tenure is to 'operationalize' privacy awareness and best practices throughout DHS, working not only with Secretary Ridge and our senior policy leadership of the various agencies and directorates of the department, but also with our Privacy Act and FOIA teams, as well as operational staff across the Department.

Consistent Policies and Education Efforts

Through internal educational outreach and the establishment of internal clearance procedures, we are sensitizing DHS directorates and components to consider privacy whenever developing new programs or revising existing ones. We are reviewing new technologies to ensure that privacy protections are incorporated in the development and implementation of these new systems. Our headquarters staff has been reviewing all Privacy Impact Assessments being conducted throughout the De-

partment. In this process, DHS professionals have become educated about to the need to consider—and the framework for considering—the privacy impact of their technology decisions. We are reviewing Privacy Act systems notices before they are sent forward and ensuring that we collect only those records that are necessary to support our mission. We also guide DHS agencies in developing appropriate privacy policies for their programs and serve as a resource for any question that may arise concerning privacy, information collection or disclosure. We work closely with various DHS policy teams, the Office of the General Counsel, and the Chief Information Officers to ensure that the mission of the Privacy Office is reflected in all DHS initiatives. And of course we also work in concert with the Department's Office for Civil Rights and Civil Liberties, which is the other statutorily mandated office at DHS Headquarters with an individual liberties focus.

Integrated Privacy and Disclosure Mandates

The work of the Privacy Office includes not only the statutory Privacy Act and Privacy Impact Assessement work, but also integrates Freedom of Information Act oversight for the Department. This additional responsibility was redelegated to the Privacy Office last summer by Secretary Ridge, in recognition of the close connection between privacy and disclosure laws, and the functional synergies of the work of our Privacy Act and FOIA specialists across the Department.

TRANSPARENCY AND OUTREACH TO THE PUBLIC

The DHS Privacy Office also seeks to anticipate and satisfy public needs and expectations, by providing a crucial link between those outside DHS who are concerned about the privacy impact of the Department's initiatives, and those inside the Department who are diligently working to achieve the Department's mission. Our role is not only to inform, educate, and lead privacy practice within the Department, but also to serve as listeners and as a receptive audience to those outside the Department who have questions or concerns about the Department's operations. To that end, my office has engaged in consistent and substantial outreach efforts to members of the advocacy community, industry representatives, other U.S. agencies, foreign governments, and most importantly, the American public, not only to inform and educate those constituencies, but also, even more importantly, to hear their concerns, to share those concerns with the Department's leadership, and to see that those concerns are addressed in our programs and in the development of our policies. Recent coverage of our privacy program, in particular our Privacy Impact Assessment, or PIA, of the US-VISIT program, demonstrated how information-collection efforts, especially those employing new or unfamiliar technology, can be done in a privacy-sensitive way. Operationally, this particular PIA demonstrated an effective internal system whereby staff from across the department worked together to create a document that was at once technologically detailed and also reader-friendly.

KEY POLICY CHALLENGES

The Use of Private-Sector Data

I can think of no more compelling public policy issue, particularly one that affects the privacy of our citizens and visitors to this country, than the sharing of personal information between the public and private sector. It is one that has been successfully—and less successfully—navigated by other agencies within the Federal government, and it is one that we examine and grapple with in programs within every single directorate and agency within the Department of Homeland Security almost every day.

It is the Privacy Office's role to facilitate this conversation about and this examination of the responsible uses of information by government agencies within DHS. That role sometimes requires us to encourage, and even force conversation between those who label themselves as being concerned only with privacy, and those who consider themselves all about security. I challenge those who feel the need to be one or the other. It is, in fact, possible, to achieve both responsible privacy practices and achieve the mission of the Department of Homeland Security. Issues of privacy and civil liberties are most successfully navigated when the necessary legal and policy protections are built in to the systems or programs from the very beginning—both in the intelligent use of technology, and in the responsible execution of programs. Further, clear rules—both in the private sector and in the public sector—are necessary to ensure that such information sharing is done in a legitimate, respectful, and limited fashion.

International Cooperation

A key focus of the Privacy Office's work has been to engage the data protection authorities internationally. Privacy professionals the world over share a common interest in assuring public trust in government operations by encouraging transparency, as well as respect for fair information principles such as collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, participation, and accountability. Our office has participated in the meetings of the International Association of Data Protection and Privacy Commissioners, although the office is not recognized at this time as an accredited data protection authority. We have also worked cooperatively with data protection authorities, or DPAs, to enable cross-border dispute resolution of personal data issues. Our office is both a point of appeals for complaints about our various directorates' programs, and also a point of contact for our international counterparts, whether acting to communicate policy concerns or individual citizens' complaints.

BALANCING THE NEED FOR TRANSPARENCY AND THE NEED FOR SECURITY IN OPERATIONS

Perhaps the most difficult issue in a law enforcement or counter-terrorism context is the need to afford transparency and access to information for individuals, while also safeguarding information that is essential to an ongoing investigation of some type. Our office seeks to assist the agency in achieving this balance in a number of ways. First, rules and procedures for accessing information must be clear, easily attainable by individuals, and easily understood. Second, determinations that information is sensitive or otherwise protected must be narrowly tailored and well grounded. Third, systems must be in place whereby individuals can be assisted in correcting information that may impact them in some way, even when that information is deemed protected. An example of this is the use of citizen advocates or ombudsmen, where by government employees who have security clearance or access to information act on behalf of individuals to correct misidentifications or incorrect information that is associated with an individual. In addition, these processes must be efficient and minimally burdensome on the individual, and must provide for an appeal or further redress process that is adequately independent to ensure fairness for the individual. These processes exist in certain places within our Department, and should be implemented where personal information is collected by the government and used in a way that impacts the individual. The DHS Privacy Office plays a role in performing that independent review and appeal process for our directorates and citizens.

THE DEFENSE OF PRIVACY ACT

The DHS Privacy Office applauds the subcommittee for its interest in privacy issues, and even more, privacy practices across the federal government. We in government are often quick to point to private-sector lapses in privacy policy, and we should be equally vigilant about our own use of personal data. While the federal government benefits from the requirements of the Privacy Act of 1974, it is also true that new technologies have allowed data sharing in new and perhaps unexpected ways. The Privacy Impact Assessment requirements of the E-Government Act of 2002 recognize these new technological challenges and seek to provide reader-friendly information about such data collections in a new and perhaps more technologically savvy fashion.

The proposed Defense of Privacy Act shares many similarities with the PIA requirements under the E-Government Act, ones that are worth noting, such as the need for a "senior agency official with primary responsibility for privacy policy." While the need for a statutory privacy officer at DHS may be virtually unique in the federal government, given the agency's size and the co-mingling of parts of more than 22 former federal agencies, the need for senior policy leadership at any agency that affects public data is certainly recognized.

Further, the Act does clarify the timing of PIAs, to be both a prospective document, issued at the NPRM stage, and a final document, issued in response to public comments. We at DHS have, and fully intend to continue to publish PIAs for public comment and we believe that this public dialogue is essential to our understanding of public concerns about DHS programs. I should note that the Administration continues to review this legislation, and we may have additional comments at a later time.

INTERNAL AND EXTERNAL ROLE

I am often asked whether I view my job as a privacy advocate and thus at odds with the activities of the Department. The answer is absolutely not. As Secretary Ridge has articulated on many occasions, the Department of Homeland Security's mission is more than just counter-terrorism, more than just the protection of people and places and things. It is also the protection of our liberties and our way of life, and that includes the ability to engage in public life with dignity, autonomy, and a general expectation of respect for personal privacy. Thus, the protection of privacy is neither an adjunct nor the antithesis to the mission of the Department of Homeland Security. Privacy protection, in fact, is at the core of that mission.

I am very much in agreement with the statutory definition of my office's position as being both "within" and "without" the Department of Homeland Security. As part of the department, we are able to serve as educators, as leaders, and as full participants in the policy direction of important programs. And as outsiders, we are able to turn a critical eye on the most controversial and the most mundane aspects of the Department's operations. But I do not position my office as the enemy of the mission of this department. Rather, I see it as crucial, fundamental to successfully achieving that mission.

On a daily basis, I am aware of what it means to set parameters for the federal government's use of personal information—information that has been given to us in our capacity as the provider of services, as the caretaker of the public's physical security, and, most importantly, the custodian of the public's trust. Secretary Ridge has said that "Fear of government abuse of information . . . is understandable, but we cannot let it stop us from doing what is right and responsible." The antidote to fear, as he has said, "is an open, fair, and transparent process that guarantees the protection and the privacy of that data." I commit to this Committee, to the American people whom we serve, and to our neighbors around the globe, that the Privacy Office is implementing this philosophy on a daily basis at the Department of Homeland Security.

I thank you for your time, and for your interest in and support of the Department of Homeland Security Privacy Office.

Mr. CANNON. Thank you.

We appreciate the exceptional job you're doing and point out that it's actually historic since other people are going to look at what you have done. And I appreciate that attitude that things exactly work better when you think about the privacy implications in advance.

Governor Gilmore, you'll be recognized for 5 minutes.

STATEMENT OF HONORABLE JAMES S. GILMORE, III, PRESIDENT, USA SECURE CORPORATION, WASHINGTON, DC

Mr. GILMORE. Chairman Cannon and Ranking Member Watt and Members of the Subcommittee, thank you for the opportunity to be here to talk to you today. I'm acquainted with most all the Members and it's a pleasure to be back here with all of you again.

A copy of my statement is put into the record, I believe.

Mr. Chairman, I'm going to—I don't typically come back to Congress these days and read a lot of things. But I think I might this time because I put this together and well, I kind of like it. So I think I'm going to read it to you, at least part of it to you.

I want to applaud the Committee for its leadership in this key area. It's been my privilege to serve as Chairman of the Advisory Panel to Assess Domestic Response Capabilities Involving Terrorism and Weapons of Mass Destruction for this Congress and reporting to this Congress and to the president for the past 5 years.

In my private business and in my law practice I represent clients in homeland security matters. I'm president of an organization called USA Secure, which the Chairman made reference to. It's a

private group of companies that come together and right now it's working mostly in bioterrorism issues.

But my main attention over the past 5 years has been as Chairman of the Advisory Panel on behalf of this Congress.

In the history of this panel we've produced five advisory reports to the Congress and to the president. The first report, in 1999, assessed the threat. The second report, in 2000, developed the fundamentals of a national strategy. The third report was dedicated to one of our members who died at the World Trade Center and went through key subject areas. The fourth report continued to fill out the idea of a national strategy focusing particularly on intelligence gathering and intelligence sharing.

And the last report, which we just issued to you on December the 15 of this past year, tries to express some end vision about where we're trying to be and with regard to a national strategy, and also focuses a great deal on the issue, frankly, of the civil freedoms of the country because of an abiding concern of the panel as we go at the door on that issue.

Today I'm here to speak to you for just a moment about the Privacy Officer position at the Department of Homeland Security. With the leadership of this Committee and the Subcommittee and the Department of Homeland Security, it has established a position of Privacy Officer in accordance with your statute. The foundation of the Congress' thinking was the protection of privacy will enhance the protection of American freedom. And as such, the primary responsibility for this policy includes oversight of the use of technologies to make sure they sustain and don't erode privacy protections, and puts a special emphasis on the Privacy Act.

In its drive to make the country more secure the United States is applying all of its managerial and technological expertise to the creation of security in the homeland. Now these are enormously powerful forces because of this highly managerial society that we're in and also that we are the greatest technological society developed in the history of mankind as has been demonstrated by this gigantic war-making capacity that we have just seen.

These twin forces of management and technology applied to homeland security can be applied to create a very secure society. But without institutional checks and balances it may override the traditional constitutional protections in this country.

Many might argue that our traditional values of privacy, anonymity, and freedom are out of date and rendered obsolete by the terrorist threat.

As chairman of the Advisory Panel and as a private citizen, I could not more emphatically disagree with the concepts that our freedoms must take second place as against the goal of creating greater security in the United States. The Congress, through this Committee and the Subcommittee, has agreed by enshrining the Privacy Officer within the statute establishing the Department of Homeland Security.

Now I want to congratulate Secretary Ridge and his Department for supporting the Privacy Officer and empowering her as greatly as they have. Through the first Privacy Officer, Nuala O'Connor Kelly, this Department contains an instinct toward the creation of a culture of privacy that will allow the personal data of people to

remain as confidential as possible within an environment of trying to weed out stealth attacks.

Now we've got laws to protect the confidentiality of private citizens, but how does the American citizen know that his confidential and private information will not be made public or even disseminated to other agencies or other organizations to disempower him by impinging upon his private information? We live in the society of the anonymous but cannot continue the society of the empowered individual if the Government has the ability to take all of the private information and then to handle that information in such a way to expose personal information.

We have long tradition of the independence of the American citizen. Now this can't continue either without systematic thinking and advocacy by someone in Government to preserve the freedoms and values of the American people. This is the duty of the Congress primarily and those of the Executive Branch who are so clearly dedicated to those freedoms. To provide that check institutionally within the Executive Branch, the Congress has provided for the Privacy Officer.

I've worked very closely with Ms. O'Connor Kelly and the Department on these issues. Their dedication to the privacy of the American people is extraordinary. Their proactive ability to inject herself into these issues is essential and real. And the office provides a check against bulling ahead to create security while running over the privacies and the freedoms of the American people. And I congratulate the Committee, the Subcommittee, the Congress, and the Department for doing that.

I urge upon the Congress we may be entering into a historic time in which bad decisions now may have consequences to the freedoms of the American people throughout the future. Privacy is an essential element of American liberty. The ability to keep personal information secure from prying eyes gives the mental empowerment to people to live as free citizens. Without that security American citizens are vulnerable and insecure, never knowing whether their personal information will be put into the hands of someone who will use that information against their interests, to make them weaker, or to destroy their individuality. Now this debate goes to the fundamental relationship between citizens and Government and ultimately will go beyond the simple issue of privacy.

In closing, we're engaged in a debate of the American citizens' roll in his own society within the context of terrorism and security. Some societies have always been more comfortable with the citizen fitting into the entire community and being subject to identification cards, reporting requirements, stops by police, the presentation of papers, subjecting citizens to interrogation, checkpoints, frisking, and prying into the personal business of citizens more than the United States has ever been willing to tolerate.

The fundamental question that the Congress must ask is whether this view of the individual is the future of the United States. The American tradition has been much more focused on the individual and his role in society. The individual has never been a creature of the Government or the entire State but relies upon the State to create an environment which he can grow on his own, es-

tablish his independence, and exist without the permission of the Government or the overall State.

The question the Congress has to answer as they consider this and other pieces of legislation is did the enemy fundamentally change the American relationship because of its attacks on September 11? This is the debate that will go forward in the years ahead. But in the meantime, I congratulate this Congress and the Department for the creation of the Privacy Officer and giving her the ability to go into these issues and to safeguard these liberties in this highly risky moment in American history.

[The prepared statement of Mr. Gilmore follows:]

PREPARED STATEMENT OF GOVERNOR JAMES S. GILMORE, III

Chairman Cannon, Ranking Member Watt, and members of the Subcommittee on Commercial and Administrative Law. The Committee on the Judiciary and the Subcommittee have played a major leadership role in including privacy considerations in the overall development of the Department of Homeland Security. I applaud the Committee for its leadership in this key area. It has been my privilege to serve as the Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction for the past five years. In my private business and law practice I represent clients in homeland security matters. I also am President of USA Secure, a group of private sector companies and non-profit organizations that come together to deal with significant homeland security issues. USA Secure's primary focus has been on bioterrorism issues to this date. My main attention in homeland security over the past five years has been as Chairman of the Advisory Panel on behalf of this Congress.

CONGRESSIONAL MANDATE

The Advisory Panel was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (H.R. 3616, 105thCongress, 2nd Session) (October 17, 1998). That Act directed the Advisory Panel to accomplish several specific tasks. It said:

The panel shall—

1. Assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;
2. Assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;
3. Assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;
4. Recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and
5. Assess the appropriate roles of State and local government in funding effective local response capabilities.

That Act required the Advisory Panel to report its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction to the President and the Congress three times during the course of the Advisory Panel's deliberations—on December 15 in 1999, 2000, and 2001.

The Advisory Panel's tenure was extended for two years in accordance with Section 1514 of the National Defense Authorization Act for Fiscal Year 2002 (S. 1358, Public Law 107–107, 107th Congress, First Session), which was signed into law by the President on December 28, 2001. By virtue of that legislation, the panel was required to submit two additional reports—one on December 15 of 2002, and one on December 15, 2003.

ADVISORY PANEL COMPOSITION

Mister Chairman, please allow me to pay special tribute to the men and women who serve on our panel.

This Advisory Panel is unique in one very important way. It is not the typical national "blue ribbon" panel, which in most cases historically have been composed almost exclusively of what I will refer to as "Washington Insiders"—people who have spent most of their professional careers inside the Beltway. This panel has a sprinkling of that kind of experience—a former Member of Congress and Secretary of the Army, a former State Department Ambassador-at-Large for Counterterrorism, a former senior executive from the CIA and the FBI, a former senior member of the Intelligence Community, the former head of a national academy on public health, two retired flag-rank military officers, a former senior executive in a non-governmental charitable organization, and the head of a national law enforcement foundation. But what truly makes this panel special and, therefore, causes its pronouncement to carry significantly more weight, is the contribution from the members of the panel from the rest of the country:

- Three directors of state emergency management agencies, from California, Iowa, and Indiana, two of whom now also serve their Governor's as Homeland Security Advisors
- The deputy director of a state homeland security agency
- A state epidemiologist and director of a state public health agency
- A former city manager of a mid-size city
- The chief of police of a suburban city in a major metropolitan area
- Senior professional and volunteer fire fighters
- A senior emergency medical services officer of a major metropolitan area
- And, of course—in the person of your witness—a former State governor

These are representatives of the true "first responders"—those heroic men and women who put their lives on the line every day for the public health and safety of all Americans. Moreover, so many of these panel members are also national leaders in their professions: our EMS member is a past president of the national association of emergency medical technicians; one of our emergency managers is the past president of her national association; our law officer now is president of the international association of chiefs of police; our epidemiologist is past president of her professional organization; one of our local firefighters is chair of the terrorism committee of the international association of fire chiefs; the other is chair of the prestigious national Interagency Board for Equipment Standardization and Inter-Operability.

Those attacks continue to carry much poignancy for us, because of the direct loss to the panel. Ray Downey, Department Deputy Chief and chief-in-charge of Special Operations Command, Fire Department of the City of New York, perished in the collapse of the second tower in the September 11 attack on the New York World Trade Center.

PANEL REPORTS

In the history of the Panel, we have produced five advisory reports to the Congress and to the President of the United State. The first report in 1999 assessed threat. The second report in 2000 developed the fundamentals of a national strategy for combating terrorism. The third report, dedicated to Ray Downey who lost his life in the World Trade Center, filled out a national strategy in five key subject areas: state and local response capabilities, health and medical capabilities, immigration and border control, cybersecurity, and use of the military. Our fourth report in 2002, issued in the year following the 9/11 attacks, further made recommendations on how to marshal the national effort towards a national strategy. It paid special attention to the needs of intelligence sharing and the proper structure for counterterrorism activities inside the United States. Our last report was issued about one and a half months ago, on December 15, 2003. That final report sought to express some end-vision and direction for the United States as it develops its national strategy and makes the country safer.

FIFTH REPORT (2003)— FORGING AMERICA'S NEW NORMALCY:
SECURING OUR HOMELAND, PRESERVING OUR LIBERTY

Mister Chairman, the Advisory Panel released its fifth and final report on December 15, 2003. In that report, the strategic vision, themes, and recommendations were motivated by the unanimous view of the panel that its final report should attempt to define a future state of security against terrorism—one that the panel has chosen to call "America's New Normalcy."

- That *strategic vision* offered by the panel reflects the guiding principles that the panel has consistently enumerated throughout its reports:
- It must be truly national in scope, not just Federal.
- It should build on the existing emergency response system within an all-hazards framework.
- It should be fully resourced with priorities based on risk.
- It should be based on measurable performance.
- It should be truly comprehensive, encompassing the full spectrum of awareness, prevention, preparedness, response, and recovery against domestic and international threats against our physical, economic and societal well-being.
- It should include psychological preparedness.
- It should be institutionalized and sustained.
- It should be responsive to requirements from and fully coordinated with State and local officials and the private sector as partners throughout the development, implementation, and sustainment process.
- It should include a clear process for strategic communications and community involvement.
- It must preserve civil liberties.

In developing the report, panel members all agreed at the outset that it could not postulate, as part of its vision, a return to a pre-September 11 "normal." The threats from terrorism are now recognized to be a condition that we must face far into the future. It was the panel's firm intention to articulate a vision of the future that subjects terrorism to a logical place in the array of threats from other sources that the American people face every day—from natural diseases and other illnesses to crime and traffic and other accidents, to mention a few. The panel firmly believes that terrorism must be put in the context of the other risks we face, and that resources should be prioritized and allocated to that variety of risks in logical fashion.

The panel has proffered a view of the future—five years hence—that it believes offers a reasonable, measurable, and attainable benchmark. It believes that, in the current absence of longer-term measurable goals, this benchmark can provide government at all levels, the private sector, and our citizens a set of objectives for readiness and preparedness. The panel did not claim that the objectives presented in this future view are all encompassing. Neither do they necessarily reflect the full continuum of advances that America may accomplish or the successes that its enemies may realize in the next five years. The view is a snapshot in time for the purpose of guiding the actions of today and a roadmap for the future.

The panel said that America's new normalcy in January of 2009 should reflect:

- Both the sustainment and further **empowerment of individual freedoms** in the context of measurable advances that secure the homeland.
- Consistent **commitment of resources** that improve the ability of all levels of government, the private sector, and our citizens to prevent terrorist attacks and, if warranted, to respond and recover effectively to the full range of threats faced by the nation.
- A standardized and effective process for **sharing information and intelligence** among all stakeholders—one built on moving actionable information to the broadest possible audience rapidly, and allowing for heightened security with minimal undesirable economic and societal consequences.
- Strong **preparedness and readiness across State and local government and the private sector** with corresponding processes that provide an enterprise-wide national capacity to plan, equip, train, and exercise against measurable standards.
- Clear definition about the roles, responsibilities, and **acceptable uses of the military domestically**—that strengthens the role of the National Guard and Federal Reserve Components for any domestic mission and ensures that America's leaders will never be confronted with competing choices of using the military to respond to a domestic emergency versus the need to project our strength globally to defeat those who would seek to do us harm.
- Clear processes for engaging academia, business, all levels of government, and others in rapidly developing and implementing **research, development, and standards** across technology, public policy, and other areas needed to secure the homeland—a process that focuses efforts on real versus perceived needs.

- Well-understood and shared process, plans, and incentives for **protecting the nation's critical infrastructures** of government and in the private sector—a unified approach to managing our risks.

The panel's *Future Vision 2009* included specifics details involving:

- ***State, Local, and Private Sector Empowerment***
- ***Intelligence***
- ***Information Sharing***
- ***Training, Exercising, Equipping, and Related Standards***
- ***Enhanced Critical Infrastructure Protection***
- ***Research and Development, and Related Standards***
- ***Role of the Military***

To support its strategic vision, the panel offered a "Roadmap for the Future," in which it made 20 substantive recommendations in six areas. (Advisory Panel recommendations are highlighted below in ***bold italics***).

CIVIL LIBERTIES AT THE FOUNDATION

The panel addressed the on-going debate in the United States about the tradeoffs between security and civil liberties. It concluded that history teaches, however, that the debate about finding the right "balance" between security and civil liberties is misleading, that the traditional debate implies that security and liberty are competing values and are mutually exclusive. It assumes that our liberties make us vulnerable and if we will give up some of these liberties, at least temporarily, we will be more secure. It concluded that civil liberties and security are mutually reinforcing. The panel said that we must, therefore, evaluate each initiative along with the combined effect of *all* initiatives to combat terrorism in terms of how well they preserve all of the "unalienable rights" that the founders believed were essential to the strength and security of our nation—rights that have become so imbedded in our society and ingrained in our psyche that we must take special precautions, take extra steps, to ensure that we do not cross the line. It is more than the clearly defined protections in the Constitution—protections against unreasonable search and seizure; and against self-incrimination. It is also that less well-defined but nevertheless exceptionally important "right to privacy" that we have come to expect and that our judicial system has come increasingly to recognize. ***We recommend that the President establish an independent, bipartisan civil liberties oversight board to provide advice on any change to statutory or regulatory authority or implementing procedures for combating terrorism that has or may have civil liberties implications (even from unintended consequences).***

THE PRIVACY OFFICER

With the leadership of this Committee and Subcommittee, the Department of Homeland Security has established the position of Privacy Officer in accordance with statute. The foundation of the Congress's thinking was the protection of privacy will enhance the protection of American freedom. As such, the primary responsibility for the privacy policy includes an oversight of the use of technologies to make sure that they sustain and do not erode privacy protections relating to the collection and disclosure of personal information. It places special emphasis on the Privacy Act of 1974 and empowers the Privacy Officer to evaluate legislative and regulatory proposals involving the disclosure of personal information.

In its drive to make the country secure, the United States is applying all of its managerial and technological expertise to the creation of national security in the homeland. These are enormously powerful forces because of the highly managerial society that the United States is today. The United States is also the greatest technologically developed society in the history of mankind as has been demonstrated by our gigantic war-making capacity. These twin forces of management and technology, applied to the homeland security issue, can be applied to create a very secure society, but without institutional checks and balances, may override our traditional Constitutional protections.

Many might quickly argue that our traditional values of privacy, anonymity, and freedom are out of date and rendered obsolete by the terrorist threat. As Chairman of the Advisory Panel, and as a private citizen, I could not more emphatically disagree with the concept that our freedoms must take second place as against the goal of creating greater security in the United States. The Congress, through this Committee and Subcommittee, has agreed by enshrining the Privacy Officer within the statute establishing the Department of Homeland Security.

I congratulate Secretary Ridge and his Department for supporting the Privacy Officer and empowering her so greatly. Through its first Privacy Officer, Nuala O'Connor Kelly, the Department contains an instinct towards the creation of a "culture of privacy" that will allow the personal data of people to remain as confidential as possible with an environment of trying to weed out stealth attacks by anonymous terrorists. We have laws to protect the confidentiality of private information of the American citizen; but, how does the American citizen know that his confidential and private information will not be made public or even disseminated to other governmental agencies or other organizations to disempower him by impinging upon his private information. We live in the culture of the anonymous leak, but we cannot continue the society of the empowered individual if government has the ability to take all of their private information and then to handle that information in such a way that citizens' private information is exposed.

We have a long tradition of the independence of the American citizen. This, too, cannot continue without systematic thinking and advocacy by someone in government to preserve the freedoms and values of the American people. This is fundamentally and primarily the duty of the United States Congress—the elected representatives of the people and the members of the Executive Branch who are so clearly dedicated to those freedoms. To provide that check institutionally within the Executive Branch, the Congress has provided for the Privacy Officer. In the course of my official capacity and my private capacity I have had ongoing communications with Nuala O'Connor Kelly and the Department of Homeland Security on these issues. Ms. Kelly and her Office's dedication to the privacy of the American people is extraordinary and solid. Her proactive ability to inject herself into these issues and the policy formation process within the department is essential. The very existence of her Office provides a check against bulling ahead to create security while running over the privacies and freedoms of the American people, and I congratulate the Committee, the Subcommittee, and the United States Congress and the Department of Homeland Security for the foresight to build in this institutional check and balance.

I urge upon the Congress that we may be entering into a historic time in which bad decisions now may have consequences to the freedoms of the American people throughout their future. Privacy is an essential element of American liberty. The ability to keep personal information secure from prying eyes gives the mental empowerment to people to live as free citizens. Without that security American citizens are vulnerable and insecure, never knowing whether their personal information will be put into the hands of someone who will use that information against their interests to make them weaker or to destroy their individuality. This debate, now, goes to the fundamental relationship between citizens and government, and should, and ultimately will, go far beyond just the issue of privacy.

We are now engaged in a debate of the American citizen's role in his own society within the context of terrorism and security. Some societies have always been much more comfortable with the citizen fitting into the entire community and being subject to the entire community or the state. As such, identification cards, reporting requirements, stops by police, the presentation of papers, subjecting citizens to interrogation, checkpoints, frisking, and prying into the personal business of citizens has always been much more accepted in many countries of the world than in the United States.

The fundamental question the Congress must ask is whether this view of the individual is the future of the United States. The American tradition has been much more focused on the individual and his role in society. The individual has never been a creature of the government or the entire state, but relies upon the state to create an environment in which he can grow on his own, establish his independence, and exist without the permission of the government or of the overall state.

Did the enemy fundamentally redefine the American relationship because of its attacks on September 11, 2001? This is the policy debate for the years ahead as we reach for further security inside the homeland. In the meanwhile, the Privacy Officer and her office represent a fundamental protection while this debate is going on. By virtue of her official duty and position, she facilitates this dialogue with the American people and helps to safeguard their liberties in this highly risky moment in American history. It is my pleasure to be here today to endorse the role of the Privacy Officer and the offices established within the Department.

Mr. CANNON. Thank you, Governor. We appreciate your service chairing that committee.

Ms. Katzen?

STATEMENT OF SALLY KATZEN, VISITING PROFESSOR, UNIVERSITY OF MICHIGAN LAW SCHOOL, ANN ARBOR, MI

Ms. KATZEN. Thank you, Mr. Chairman, Ranking Member Watt, Members of the Committee. I appreciate very much your inviting me to testify today on a subject of interest to millions of Americans.

As the Chairman noted, the views that I am expressing are my own and not those of any of the entities which may I may be affiliated.

This Committee is indeed to be congratulated, not only for its leadership in creating a statutory Privacy Officer in the Department of Homeland Security, but also for being vigilant in its oversight of that office. Given the Committee's extensive experience in this area, it is not necessary to speak at length on the centrality of privacy in our country. It is a value that has been cherished, prized, protected and defended throughout our country and throughout history.

Before September 11, 2001, privacy concerns polled off the charts. Since then Americans have acknowledged the importance of security and the need for combating terrorism, but their commitment to privacy has not been diminished. And some would argue, with much force, that if in protecting our Nation we're not able to preserve a free and open society for public lives with commensurate respect for the privacy of our personal lives, then perhaps the terrorists will have won.

For that reason, again, I believe it was necessary and desirable to create a Privacy Officer within the Department of Homeland Security. Ms. Kelly has been there for approximately a year and we have heard this afternoon about her qualifications, which are genuinely impressive, and her activities to date, the earliest signs of which are indeed encouraging. And I will not try to repeat any of that.

I draw two lessons from Ms. Kelly's tenure at DHS. First, the existence of a statutory Privacy Officer is highly beneficial. We now know that some attention is being paid to privacy concerns and steps are being taken to advance this important value that might otherwise not have occurred.

The Chairman mentioned the CAPPS II project. There she inherited a Privacy Act notice that was issued last winter that was dreadful and she greatly improved it. In my written testimony I suggest some areas where additional work could, I believe should, be done to make it even better.

I also talk about the US-VISIT program and again would refer you to my written testimony.

But there is no doubt that the work that she has done has been good and is highly beneficial.

Now as someone outside the Government, it is hard to know how influential she will be if, and it inevitably will happen, there is a direct conflict between what a program office wants and what she counsels against.

Secretary Ridge has said all of the right things in supporting the Privacy Officer and we know he can do well in that regard. But we do not know what will happen when the rubber hits the road. This Committee, however, can further empower the Privacy Officer and lay the foundations for remedying any problems that may arise by

maintaining its oversight and inquiring pointedly into how the Department handles these issues.

The second lesson that I would take from the experience to date with the Privacy Officer at DHS is that there has been no diminution in the capacity of the Department to fulfill and pursue its mission. This is wholly consistent with what most Americans think, that national security and privacy are compatible.

Now the fact that there is no evidence that the existence or any activity of the Privacy Officer has caused DHS to falter leads me to suggest that the Committee consider expanding the number of statutory privacy officers from one to 24, covering all of the major departments, or at least a handful of critical agencies.

I mean, imagine the salutary effect that a privacy officer who is statutorily empowered could have at the Department of Justice, the Treasury, the IRS, DOD and VA, SSA, and HHS. All of these have some sort of privacy officer in place but they are, for the most part, processing Privacy Act complaints and not being involved in the underlying activities of their agencies and their departments.

I would go one step further and suggest, indeed strongly urge, that you create a statutory privacy office at OMB, an office headed, as we called it in the Clinton administration, by the chief counselor for privacy. We had such an office and it served us well. In my written testimony I give you the range of ideas and subjects that have been—that were discussed.

I believe it is unfortunate that the current Administration has chosen not to fill that position. As a result, there is no senior official in the Executive Office of the President who has privacy in his or her title or who is charged with oversight of Federal privacy practices, monitoring of interagency processes where privacy is implicated, or developing national privacy policies.

Perhaps it was the absence of such a person that led the Bush administration to its initial lack of support for the designation of a Privacy Officer at DHS, which it has now come to embrace. Perhaps if someone had been appointed to the position, the Administration would not appear to some to be so tone deaf to privacy concerns in such areas as the PATRIOT Act or any other number of law enforcement issues that have appeared in the papers over the last several years.

An office inside OMB can provide both institutional memory and sensitivity to combat the unfortunate tendency of some within Government to surveil first and think later.

I have also in my written testimony a series of comments on the bill that I hope you will have a chance to review. And again, I thank you for your kind attention and look forward to responding to any questions you might have.

[The prepared statement of Ms. Katzen follows:[

PREPARED STATEMENT OF SALLY KATZEN

Thank you for inviting me to testify today on a vitally important subject—"Privacy in the Hands of the Government." This Committee is to be congratulated, not only for its leadership in creating a statutory Privacy Officer in the Department of Homeland Security (DHS), but also for being vigilant in its oversight of that office.

I am currently a Visiting Professor at the University of Michigan Law School, where one of my courses is a seminar on "Technology Policy in the Information Age"—a significant portion of which is devoted to examining both the government and the private sector's privacy policies and practices. I have been involved in pri-

vacy policy for over a decade. In early 1993, I began serving as the Administrator of the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB); the "I" in OIRA signaled that I was, in effect, the chief information policy official for the federal government. Among other responsibilities, my office was charged with developing federal privacy policies, including implementation of the 1974 Privacy Act. Later in 1993, I was asked to chair the Information Policy Committee of the National Information Infrastructure Task Force, which had been convened by the Vice President and chaired by then Secretary of Commerce Ronald Brown. One of the first deliverables we produced was from my committee's Privacy Working Group—a revision of the 1973 Code of Fair Information Practices, entitled "Principles for Providing and Using Personal Information." During President Clinton's second term, I worked with the Vice President's Domestic Policy Advisor to create a highly visible and effective office for privacy advocacy in OMB; we selected Peter Swire to head that office and be the first Chief Counselor for Privacy, and I worked closely with him when I served as Deputy Director for Management at OMB during the last two years of the Clinton Administration. Since leaving government, I have, as indicated earlier, been teaching both at the graduate and undergraduate level.

Given the Committee's extensive work in this area, it is not necessary to speak at length on the importance of privacy in the history and culture of our country. Nonetheless, to provide context for the comments that follow, I want to be clear that, from my perspective, privacy is one of the core values of what we are as Americans. Whether you trace its roots from the first settlers and the "frontier" mentality of the early pioneers, or from the legal doctrines that flowed from Justice Brandeis' oft-quoted recognition in the late 19th century of "the right to be let alone," privacy has been one of the hallmarks of America—cherished, prized, protected and defended throughout our country and throughout our history.

The "Information Age" has brought new opportunities to benefit from the free flow of information, but at the same time it has also raised privacy concerns to a new level. Computers and networks can assemble, organize and analyze data from disparate sources at a speed (and with an accuracy) that was unimaginable only a few decades ago. And as the capacity—of both the government and the private sector—to obtain and mine data has increased, Americans have felt more threatened—indeed, alarmed—at the potential for invasion (and exploitation) of their privacy.

Before September 11, 2001, privacy concerns polled off the charts. Since then, there has been a recognition of the importance of security and the need for combating terrorism. But, as the Pew Internet surveys (and others) have found, Americans' commitment to privacy has not diminished, and some would argue (with much force) that if, in protecting our nation, we are not able to preserve a free and open society for our public lives, with commensurate respect for the privacy of our private lives, then the terrorists will have won. For that reason, it was both necessary and desirable in creating a Department of Homeland Security to statutorily require the Secretary to appoint a senior official with primary responsibility for privacy policy. Ms. Kelly was selected for that position and took office about six months ago.

We thus have some—albeit limited—operational experience with the statutory scheme, and it is therefore timely to see what we have learned and what more could (and should) be done by this Committee to be responsive to privacy concerns.

I would draw two lessons from Ms. Kelly's tenure to date at DHS.

First, the existence of a Privacy Officer at DHS, especially someone who comes to the position with extensive knowledge of the issues and practical experience with the federal government, is highly beneficial. We know that some attention is now being paid to privacy concerns and that steps are being taken to advance this important value that might otherwise not have occurred.

Consider the CAPPS II project, in which Ms. Kelly has recently been involved. She inherited a Privacy Act Notice issued last winter that was dreadful. She produced a Second Privacy Act Notice that reflected much more careful thought about citizens' rights and provided more transparency about the process. Regrettably, there was some backsliding: the initial concept was that the information would be used only to combat terrorism, whereas the second Notice indicated that the information would be used not only for terrorism but also for any violation of criminal or immigration law. Also, the document was vague (at best) on an individual's ability to access the data and to have corrections made. And there was more that should have been said about the manner in which the information is processed through the various data bases. But there is no question that the Second Notice was greatly improved from the first.

Ms. Kelly was also involved with the US VISIT program, where she produced a Privacy Impact Analysis (PIA). Some had argued that a PIA was not required because the program did not directly affect American citizens or permanent residents.

Nonetheless, to her credit, she prepared and issued a PIA that was quite thoughtful and was well received. Whether one agrees or disagrees with the underlying program, at least we know that someone was engaged in the issues that deserve attention and the product of that effort was released to the public.

As someone outside the government, it is hard to know how influential Ms. Kelly will be if—and it inevitably will happen—there is a direct conflict between what a program office within DHS wants to do and what the Privacy Officer would counsel against for privacy reasons. Effectiveness in this type of position depends on autonomy and authority—that is, on the aggressiveness of the office holder to call attention to potential problems and on support from the top. We may take some comfort from Secretary Ridge's comments; he has said all the right things about supporting the Privacy Officer. But we cannot now know what will happen when the "rubber meets the road."

This Committee, however, can further empower the Privacy Officer, and lay the foundation for remedying any problems that may arise, by maintaining its oversight and inquiring pointedly into how the Department operates. For example, Ms. Kelly (and Secretary Ridge) should be asked at what stage she is alerted to or brought into new initiatives; what avenues are open for her to raise any questions or concerns; and whether the Secretary will be personally involved in resolving any dispute in which she is involved. The timing of the release of the PIA for the US VISIT program suggests that Ms. Kelly may not always be consulted on a timely basis. As I read the E-Government Act of 2002, an agency is to issue a PIA *before it develops or procures* information technology that collects, maintains or disseminates information that is in an identifiable form. In this instance, the PIA was released much further down the road, when the program was about to go on line. Anything that helps the Privacy Officer become involved in new initiatives at the outset, before there is substantial staff (let alone money) invested in a project, would be highly salutary.

The second lesson that I take from the experience to date with the Privacy Officer at DHS is that there has been no diminution in the capacity of the Department to pursue its mission. Or as a political wag would say, the existence of a Privacy Officer in DHS has not caused the collapse of western civilization as we know it. This is wholly consistent with what most Americans think—that national security and privacy are compatible and are not intrinsically mutually exclusive.

The fact that there is no evidence that the existence, or any activity, of the Privacy Officer has caused DHS to falter leads me to suggest that the Committee consider expanding the number of statutory privacy offices from one to 24, covering all major Departments (the so-called Chief Financial Officers Act agencies) or at least a handful of critical agencies. Imagine the salutary effect that a statutory privacy office could have at the Department of Justice, the Department of the Treasury (and the Internal Revenue Service), the Department of Defense and the Veterans Administration, the Social Security Administration, and the Department of Health and Human Services. All of these agencies already have some form of privacy office in place, although many simply process Privacy Act complaints, requests, notices, etc. and do not involve themselves in the privacy implications of activities undertaken by their agencies. It is significant, I believe, that OMB guidance from two administrations (issued first during the Clinton Administration and repeated recently by the Bush Administration) has called for the creation of such offices in Executive Branch agencies. With the imprimatur of Congress, these offices can achieve the status (and increased influence) and gain the respect that the Privacy Officer has enjoyed at DHS. Equally important, by establishing statutory privacy offices, the Congress will be able to engage in systematic oversight of the attention paid to this important value in the federal government—something which has not occurred before this hearing today.

I hope I do not seem presumptuous to suggest—indeed, strongly urge—one further step: establishing at OMB a statutory office headed by a Chief Counselor for Privacy. As noted above, we had created such a position during the Clinton Administration, and it served us well. Peter Swire, the person we selected to head that office, was able to bring his knowledge, insights, and sensitivity to privacy concerns to a wide range of subjects. In his two years as Chief Counselor, he worked on a number of difficult issues, including privacy policies (and the role of cookies) on government websites, encryption, medical records privacy regulations, use and abuse of social security numbers, and genetic discrimination in federal hiring and promotion decisions, to name just some of the subjects that came from various federal agencies. He was also instrumental in helping us formulate national privacy policies that arose in connection with such matters as the financial modernization bill, proposed legislation to regulate internet privacy, and the European Union's Data Protection Directive.

I believe it is unfortunate that the current Administration has chosen not to fill that position. As a result, there is no senior official in the Executive Office of the President who has "privacy" in his/her title or who is charged with oversight of federal privacy practices, monitoring of interagency processes where privacy is implicated, or developing national privacy polices. Perhaps it was the absence of such a person that led to the Bush Administration's initial lack of support for the designation of a Privacy Officer at the Department of Homeland Security. Perhaps if someone had been appointed to that position, the Administration would not have appeared to be so tone deaf to privacy concerns in connection with the Patriot Act or any number of law enforcement issues that have made headlines over the past several years. An "insider" can provide both institutional memory and sensitivity to counterbalance the unfortunate tendency of some within the government to surveil first and think later. At the least, the appointment of a highly qualified privacy guru at OMB would mean that someone in a senior position, with visibility, would be thinking about these issues before—rather than after—policies are announced.

Finally, I understand that after this Hearing, the Committee will move to mark up H.R. 338, "The Defense of Privacy Act." That bill reflects a commendable desire to ensure that privacy impact statements are prepared by federal agencies as they develop regulations which may have a significant privacy impact on an individual or have a privacy impact on a substantial number of individuals. I was struck in reviewing the E-Government Act of 2002 for this testimony that it requires an agency to prepare a PIA not only before it develops or procures information technology that implicates privacy concerns, but also before the agency initiates a new collection of information that will use information technology to collect, maintain or disseminate any information in an identifiable form. This law has gone into effect, OMB has already issued guidance on how to prepare the requisite PIAs, and the agencies are learning how to prepare these PIAs using that model. Rather than impose another regime on agencies when they are developing regulations (which are frequently the basis for the information collection requests referenced in the E-Government Act of 2002), it might be preferable to amend the E-Government Act to expand its requirements to apply to regulations that implicate privacy concerns. That approach would have the added benefit of eliminating the inevitable debate over the judicial review provisions of H.R. 338, which go significantly beyond the judicial review provisions of any of the comparable acts (e.g., Reg.Flex., NEPA, Unfunded Mandates, etc.). Lastly, if you were to amend the E-Government Act to include privacy-related regulations, you might also consider including privacy-related legislative proposals from the Administration. As you know, Executive Branch proposals for legislation are reviewed by OMB before they are submitted to the Congress. If there were a Chief Counselor for Privacy at OMB, s/he would be able to provide input for the benefit of the Administration, the Congress and the American people.

Again, thank you for inviting me to testify today. This Committee has been an effective leader on privacy issues, and it is encouraging that you are continuing the effort. I would be pleased to elaborate on these comments or answer any questions that you may have.

Mr. CANNON. Thank you Ms. Katzen.

Mr. Dempsey, you're recognized for 5 minutes.

STATEMENT OF JAMES DEMPSEY, ESQUIRE, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC

Mr. DEMPSEY. Chairman Cannon, Ranking Member Watt, Members of the Subcommittee, thank you for this opportunity to testify today about the Privacy Officer at the Department of Homeland Security. It's always a privilege to appear before the Subcommittee, and especially today on a panel with three of the most serious and insightful public officials—public servants that I know.

Based on the record of the Department of Homeland Security Privacy Office to date, it is clear that a statutory Privacy Officer participating in senior level policy deliberations and using tools like the Privacy Act notice and privacy impact assessments can be an important mechanism for raising and mitigating privacy concerns surrounding the Government's use of personal information.

Certainly the Department of Homeland Security Privacy Officer legislation should be a model for other agencies including the Department of Justice.

With proper laws and policies, statutory privacy officers can be an important element of the overall approach to meeting the public's interest in privacy protection even as the Government pursues urgent missions like counterterrorism. And there's no more persuasive spokesperson and no more persuasive source for the proposition that we can and must protect privacy at the same time that we are pursuing the mission of counterterrorism than the five reports that Governor Gilmore has submitted to this Congress and his overall advocacy for the need to both preserve privacy and enhance our national security.

One of the best ways to protect privacy is to raise privacy concerns early in the development of any new program so that those concerns can be addressed and mitigated in advance. We call this privacy by design, building in the privacy protections from the ground up before a system is implemented and before it's too late to avoid the problem. That's one of the roles that the chief privacy officer plays, perhaps one of the primary roles that person plays.

Congress and this Committee were very foresightful when you insisted on creating a statutory Privacy Officer in the Homeland Security Act of 2002, but that so far is the only privacy officer statutorily created in the entire Government.

While this is a new position, Nuala O'Connor Kelly has set the benchmark and it is now clear that we can extend the model to other agencies.

It seems, based upon the evidence so far and the experience, that there are four elements of an effective privacy officer. One is a statutory basis. As Ms. Katzen has referenced, there are Privacy Act officers and privacy officers in other Federal agencies, but they don't have the stature that comes from a statutory basis and a statutory charter.

Second, adequate staff.

Third, inclusion in the senior level policy deliberations, which partly flows from the statutory charter.

And finally, legislative tools like the privacy impact assessment.

And on the fourth point, we should all recognize that privacy officers are part of the answer but that they cannot be effective unless the laws and policies are in place. One of those tools is the privacy impact assessment. The E-Government Act of 2002 requires that Federal agencies conduct privacy impact assessments whenever they are initiating a new collection of personal information or purchasing new technology. And one of the first PIAs was performed by the Department of Homeland Security Privacy Officer on the US-VISIT program.

Mr. Chairman, if I may, we have—the Center for Democracy and Technology filed some written comments on that privacy impact assessment and I'd like to ask that those be entered into the record.

Mr. CANNON. You can certainly just include those with your written statement.

Mr. DEMPSEY. Thank you, Mr. Chairman.

A further step is the bill that was just reported favorably by the Committee, H.R. 338. And just to second some of the comments

made by Congressman Coble and by Mr. Watt, this was not a surprise that this was going to be marked up. It was long overdue. It is legislation that I personally testified in favor of at an earlier hearing of this Subcommittee. It's time to get that moving and hopefully get it through the Senate as well.

We had some specific suggestions on improving that bill as it moves through the process and I understand the pressure to move that bill as it has previously passed the Committee, but by the time the legislative process is completed on that, I hope that you can reconcile the language in this privacy impact assessment legislation for regulations with the privacy impact assessment requirements that are in the E-Government Act. It's been hard enough getting the E-Government Act PIAs going. There's no need to have two separate sets of requirements or definitions and you really need to mesh H.R. 338 with section 208 of the E-Government Act.

Other issues Congressman Watt and other Members have alluded to need to be addressed. The Privacy Act of 1974 has not really kept pace with changing technology, particularly as we're seeing the Government increasingly turn to commercial databases in carrying out particularly its counterterrorism activities. We need to have strong guidelines on use of that kind of information, and on the sharing of that information.

And finally, we need the continued involvement of the Subcommittee through the oversight process. So with H.R. 338 you've taken another incremental step with the Privacy Officer at the Department of Homeland Security and hopefully proliferating that model through the Government is another step. And the question of the continued currency of the Privacy Act should be another issue that I believe the Committee and the Congress will need to address.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Chairman Cannon, Ranking Member Watt, Members of the Subcommittee, thank you for the opportunity to testify today about the Privacy Officer for the Department of Homeland Security. Based upon the short but significant record of that office to date, it is clear that a statutory Privacy Officer, participating in senior level policy deliberations and using the tools of Privacy Act notices and Privacy Impact Assessments, can be an important mechanism for raising and mitigating privacy concerns surrounding the government's use of personal information. Certainly, the DHS Privacy Officer legislation is a model for other agencies, including the Department of Justice. With some further reforms we support, including enactment of the Defense of Privacy Act and improvements to the Privacy Act of 1974, statutory Privacy Officers should be an important element of the overall approach to meeting the public's deeply-held and constitutionally-based interest in privacy protection even in the pursuit of urgent governmental missions like counterterrorism.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the Internet. Our core goals include enhancing privacy protections both in consumer transactions and between citizens and their government. We are also strong supporters of electronic government, having worked closely with key Members of the House and Senate for enactment of the E-Government Act of 2002. We commend you for your sustained attention to the important privacy issues associated with the government's collection and use of personal information. We look forward to ongoing work with you on these matters.

I. SUMMARY

The federal government has many legitimate needs for collection and use of personal information, ranging from administration of benefits programs to tax collection to winning the war on terrorism. Especially in light of the digital revolution, this government demand for information brings with it heightened risk to privacy and the associated values of Fair Information Practices—including notice; limits on collection, use, disclosure and retention; data quality; security; and the citizen's right to review and correct information held about himself.

One of the best ways to protect privacy, while facilitating the effective collection and use of information where necessary to carry out a governmental function, is to raise privacy concerns early in the development of a new program, so that those concerns can be addressed and mitigated in advance. We call this "privacy by design"—building in privacy protections from the ground up. Watchdog groups like CDT and even Members of Congress often find out about a privacy problem only after a system has been implemented. Then, it is often difficult to correct the problem. To ensure that privacy issues are addressed early on, many private companies and some government agencies have created a Chief Privacy Officer position—someone inside the organization, who can be consulted during the conceptualization phase of a new project involving collection of personal information.

In the Federal government, the Department of Homeland Security (DHS) has a statutorily created Privacy Officer—the only such statutory position in the U.S. government today. While this is a new position, CDT has been impressed with the role that Nuala O'Connor Kelly has assumed within the Department. We believe that the DHS experience should serve a model for agencies across the government.

We would also like to take this time to again voice our support for the Defense of Privacy Act (DOPA), which will require agencies to publish Privacy Impact Assessments (PIAs) for all regulations. DOPA will serve as a sound complement to Section 208 of the E-Government Act of 2002, which requires that federal agencies conduct PIAs whenever they purchase a new information technology or initiate a new collection of personally identifiable information. One of the first published PIAs was the one written by the DHS Privacy Officer on the US-VISIT (United States Visitor and Immigrant Status Indicator Technology) program. It is an important document and has served to bring greater transparency to that program. PIAs can be especially effective if they are published before the system design or regulatory process is completed.

II. CHIEF PRIVACY OFFICERS

A. History of Chief Privacy Officers in the Federal Government

For years, many federal agencies have had "Privacy Act Officers." In some agencies, this has actually been a part-time job. Privacy Act Officers often spend much of their time not on privacy issues per se, but in dealing with requests from individuals who want to see their government records under the access provisions of the Privacy Act. In addition, these officers usually are also responsible for the other major records disclosure law, the Freedom of Information Act. Privacy Act Officers, despite their title, have no statutory basis in the Privacy Act. There is no mechanism for including them in internal deliberations on matters affecting privacy. They are often mid-level career officials and do not have the ability to intervene at a policy level even when a major privacy issue comes to their attention. They are often brought into discussions about a program only at the last minute to draft a notice required under the Privacy Act when the government creates or changes a "system of records," but that notice generally serves no role in shaping policy.

Realizing that this system was not effective, the Clinton Administration in 1998 required all agencies to "designate a senior official within the agency to assume primary responsibility for privacy policy." [1] The Clinton Administration used these "privacy leaders" to review Privacy Act compliance within each agency. The next year, Peter Swire was named Chief Privacy Counselor for the Administration within the Office of Management and Budget. Mr. Swire worked on both commercial and government privacy issues and had a voice in deliberations concerning agencies across the government. Among his accomplishments was requiring all government Web sites to include privacy notices.

At the same time, many companies in the private sector began to hire or promote employees to be "Chief Privacy Officers." The CPO position is now very common in the e-commerce, banking and health care industries. Several membership organiza-

[1] William J. Clinton, "Memorandum for the Heads of Executive Departments and Agencies," May 14, 1998, <http://www.cdt.org/privacy/survey/presmemo.html>.

tions of CPOs have formed. The largest of these, the International Association of Privacy Professionals (IAPP), now meets twice yearly and includes a wide range of industry and government representatives from around the world.

In 2001, many of the privacy leaders within federal agencies—mostly political appointees—left government service with the change in administrations. Despite urging from privacy advocates,[2] the Bush Administration did not hire a new Chief Privacy Counselor and only a few agencies kept their privacy leaders. Some of these privacy leaders thrived in new full time roles as Chief Privacy Officers. In fact, a few of the federal government Chief Privacy Officers have been among the most innovative in the world, in either the public or private sectors.

B. Two Examples of Chief Privacy Officers in the US Federal Government

—Internal Revenue Service

After a series of hearings in the late 1990s, which exposed extraordinary privacy abuses by IRS agents, the IRS began to take privacy more seriously and appointed Peggy Irving to the position of "Privacy Advocate." Ms. Irving drew upon the Canadian model of Privacy Impact Assessments to ensure that program managers understood the privacy implications of their projects, took proper steps to protect personal information, and trained employees on the privacy aspects of new programs or systems. The Federal Chief Information Officer (CIO) Council soon recognized this model as a best practice and it became the basis for the E-Government Act's requirements for Privacy Impact Assessments as well as a model for private sector PIAs. In 2003, Ms. Irving left for a job with the federal courts and Maya Bernstein filled the Privacy Advocate position. Ms. Bernstein has already begun to take a leadership role in the privacy community and has been active in government-wide discussions on privacy policy.

—US Postal Service

The Postal Service collects a wide range of personal information from individuals in order to deliver the mail properly, yet it maintains one of the most trusted brand names among Americans.[3] In 2001, Zoë Strickland became the agency's first Chief Privacy Officer. Ms. Strickland worked with the Postal Service's CIO to reexamine the organization's Privacy Act Systems of Records and data flows within the agency, improving both efficiency and privacy simultaneously. After this process was complete, Ms. Strickland helped put together for project managers a full "business impact assessment" process that examines a wide range of potential issues, including privacy and security impact assessments. Ms. Strickland has also been a strong advocate for simplifying the often complex and legalistic privacy notices published both on Web sites and in the Federal Register. Ms. Strickland is frequently mentioned in the media as one of the top privacy officers in the world.

C. The DHS Privacy Officer

Based on these positive experiences, Congress created the first statutory privacy officer in Section 222 of the Homeland Security Act of 2002. The DHS Privacy Officer's statutory responsibilities include "evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government" and "conducting a privacy impact assessment of proposed rules of the Department . . .. including the type of personal information collected and the number of people affected." The Privacy Officer reports directly to the Secretary.

In April, 2004, Nuala O'Connor Kelly was named to the post. In CDT's opinion, Ms. Kelly was the right person for a difficult job. She had privacy sector experience dealing with a startup company that was trying to rapidly improve privacy protection while expanding its business, and she had experience within the Bush Administration as Chief Privacy Officer at the Commerce Department. She was well known to privacy advocates and industry.

In only ten months on the job, Ms. Kelly has been able to show why the Privacy Officer position is so vital to the success of the new department. She has become a trusted participant in internal agency deliberations while at the same time reaching out to privacy advocates and increasing public transparency of some of the most controversial programs in government today.

---

[2] Several privacy groups and academics including CDT wrote to OMB Director Mitch Daniels urging him to continue the position <http://www.cdt.org/privacy/010416omb.shtml>.

[3] According to a "privacy trust" survey of government agencies, industries and others conducted by Carnegie Mellon University and the Ponemon Institute, the Postal Service placed 5th of 26 categories, just above law enforcement and charitable organizations. DHS finished 25th of 26. Dr. Larry Ponemon, "In Whom Do You Trust," Darwin Magazine, November 2003. <http://www.darwinmag.com/read/110103/trust.html>.

For example, despite the tight time pressures created in the implementation of the US-VISIT program in January, DHS released a forthright and clear analysis of the privacy issues involved with the program. After the PIA was released, the Privacy Officer hosted a meeting for a wide range of privacy advocates and immigration groups with the US-VISIT team. Advocates expressed their concerns about issues such as the lack of information on redress issues for visitors who believe that information held about them may be incorrect or incorrectly interpreted and the unclear nature of the data quality and data retention rules. Ms. Kelly and the US-VISIT team promised that these issues will be actively addressed as the program moves forward.

We do have specific criticisms of the way DHS has handled privacy issues. The PIA on US-VISIT would have been far more meaningful if it had been issued before the program was actually being implemented. After all, the PIA is intended to surface privacy issues so they can be resolved with public input before a program is implemented. Ms. Kelly has stated that the agency will release future PIAs in advance of the program launch. In addition, as noted above, the US VISIT PIA was deficient on the question of redress and should have been more specific on data quality and data retention.

These criticisms should not detract from the basic point: the DHS Privacy Officer is an important institution and one that deserves support. CDT looks forward to continued work with the Privacy Officers as she actively builds an internal team and hones the tools she will need to ensure that privacy is adequately respected in all homeland security projects.

D. Statutory Authority for Privacy Officers

Based upon the DHS experience, as well as the experience at other agencies and in the private sector, CDT believes that every federal agency should have a statutory Privacy Officer with authorities similar to those provided under the Homeland Security Act. This officer would have the stature and authority to gain attention to this important issue and effectively conduct privacy impact assessments and train agency staff in their privacy responsibilities.

The essential elements of an effective Privacy Officer function, as we see it are three-fold: (1) statutory basis; (2) adequate staff; (3) inclusion in senior-level policy deliberations.

Even with these elements, the Privacy Officer is not a panacea. Congress cannot create Privacy Officers and claim to have solved the privacy problems associated with government in the digital age. Continued oversight will be needed. And the underlying statutory authorities must be strengthened. Privacy Officers alone cannot mitigate, for example, the problems associated with data mining and the blurring of the lines between government and private sector databases. That will require Congressional and Executive Branch action to detail the standards and guidelines for information access and sharing.

III. FURTHER PRIVACY REFORMS NEEDED

Privacy Officers are part of the answer to the privacy challenge, but they cannot be effective if the privacy laws remain outmoded for changing technology. The best, most effective Privacy Officer will achieve nothing if she does not have good laws to work with.

PIAs have become a key tool for Privacy Officers, Congress and the public to monitor federal programs. Under the Section 208 of the E-Government Act, signed into law by President Bush at the end of 2002, federal agencies were supposed to begin posting PIAs in April 2003. Those that have been made available have been high quality documents, yet, unfortunately, most agencies have not been making their PIAs publicly available. This is partly due to the fact that OMB only published guidance for Section 208 in November 2003. But more importantly now, OMB has encouraged agencies not to make PIAs available until after their budgets are finalized. This is inconsistent with the purpose and value of PIAs. PIAs should be released as soon as they are completed, to promote public participation in the debate over pressing privacy concerns.

There is also a need for greater awareness within government of the new privacy provisions of the E-Government Act. CDT has been working with key partners to organize a series of workshops to educate government officials on what they need to do to comply with the Act's core requirements. In April 2003, CDT co-hosted a workshop on the new privacy rules that were being drafted under the Act. Speakers included the DHS Chief Privacy Officer and representatives from OMB. In November, CDT co-hosted a public workshop to help agencies craft and review the reports on privacy activities required under Act. In 2004, we will be hosting further workshops on implementation of the E-Government Act. The first of these already took

place on January 22, when CDT co-hosted a forum to help agencies comply with the Act's provisions on machine readable privacy notices. And on March 31, CDT will be hosting, along with the Council for Excellence in Government and the American Council for Technology, a workshop on PIAs.

CDT previously testified that the Privacy Impact Assessments required under the Defense of Privacy Act will complement the PIA requirements of the E-Gov Act. We are very pleased that the Subcommittee is planning to report the bill. As DOPA moves forward, we recommend that you ensure that the PIA provisions of DOPA and the E-Government Act are congruent. Our initial thoughts are that this should be done by making the list of factors to be considered in a PIA the same in both laws, and by making it clear that when a new collection of information is initiated by rule, the notice and comment provisions of the Defense of Privacy Act apply to the privacy impact assessment process. Indeed, the publication requirement of DOPA is an improvement over the E-Government Act; it may be desirable to amend the latter to make it clear that PIAs must generally be published for comment before a system is procured or a program is implemented.

Other privacy issues that need to be addressed include the need to update the Privacy Act. One of the Act's key definitions—"system of records"—is ill-suited to the current data environment, in which much information useful to the government is held by the private sector. Under current law, the government may be able to bypass the Privacy Act by accessing existing private sector databases rather than collecting the information itself. When citizens and policymakers alike are concerned about the potential abuses of "data-mining" techniques, Congress obtain a full reporting from all agencies as to their uses of commercial databases and should insist that there be clear guidelines as to the access to and use of commercial data.

IV. CONCLUSION

CDT commends the Subcommittee for holding this important hearing. The excellent work of the DHS Chief Privacy Officer provides a vision of what could be. Privacy Officers cannot alone solve every privacy problem that will face the federal government. However, if the Privacy Officer position is statutorily chartered for each agency and if Privacy Impact Assessments are required to be published for both regulations and information collections, the public will be insured greater accountability and responsibility on this important issue.

Mr. CANNON. Thank you, Mr. Dempsey.

Without objection, I would like to recognize the sponsor and then the primary co-sponsor for questioning out of order. We'll go back to the time people arrived for questioning after that. So Mr. Chabot, the gentleman from Ohio is recognized for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman. I appreciate that very much.

Clearly, as we've seen from the testimony of all the witnesses here today, protecting the American people from terrorist threats is a paramount importance, yet protecting the civil liberties that Americans cherish and their privacy is also a critical issue. Balancing security and civil liberties in the face of terrorist threats around the world is a difficult task that must be carefully considered.

Ms. Kelly, thank you for your service at the Department of Homeland Security and for appearing before the Subcommittee today. We appreciate it very much. Your testimony will be tremendously helpful as Congress deliberates on how best to protect the privacy of our Nation's citizens

As the Chief Privacy Officer for the Department of Homeland Security—I've got a couple questions. I'll just put them all together rather than keep going over them. But you're really in a unique position to evaluate the benefits of privacy impact assessments in the Federal regulatory process.

Could you detail for the Subcommittee, this is my first question, how preparing privacy impact assessments have affected the regu-

latory process at the Department of Homeland Security? Specifically, one of the primary goals of the bill which just passed the Committee a little while ago is to urge Federal agencies to reconsider regulations that are potentially harmful to the privacy rights of the American people and ultimately pursue less intrusive alternatives.

In your experience at DHS, has the consideration of privacy rights as regulations are formulated affected the ultimate product? Or has the preparation of privacy impact statements resulted in the reconsideration of any proposed regulations or the pursuit of alternative plans?

And finally, a few concerns have been raised about the burden preparing privacy impact assessments might have on the Federal regulatory process. Have you experienced any significant burden associated with preparing privacy impact assessments at the Department of Homeland Security?

You can address them in any order that you'd like.

Ms. O'CONNOR KELLY. Thank you so much for those questions.

It is actually one of the most important programs, I think, within the Department of Homeland Security's Privacy Office, to oversee the development of privacy impact assessments for the Department. And if I might, I'd like to detail a little bit the process that we follow.

We actually have given our directorates written instructions that the program office for each of the directorates is responsible for the initial drafting of a privacy impact assessment. That makes the program officials and policymakers for each of the various 22 agencies that now make up the Department on the hook and responsible for the initial determination of whether a privacy impact assessment is required from the very beginning of an idea.

And of course, that can be done in direct consultation with my office. It should also be done in consultation with the Privacy Act and Privacy Officers within the directorate and with the chief information officers for that directorate so that privacy impact assessment requirements will be considered from the very beginning of any program development.

And of course, it should be said that the section 208 requirements skew more toward the new technology developments and new program developments rather than toward notice of proposed rulemakings as the proposed legislation does.

I would have to say that it is again one of the most important processes, I think, for the evaluation of privacy impact of any new program for the Department. It forces the analysis to occur at the earliest possible stages. And we have also endeavored to make those privacy impact assessments public so that, as your proposed legislation suggests, citizens can comment on the PIA and the proposed program at the earliest implementation or proposed stages.

So I don't see it as a burden, although if you want to talk about man-hours or person-hours, to do a good privacy impact assessment does require substantial amount of time by employees of the program office, of the Chief of Information's Office, and also of my office. But we don't necessarily see that as a negative burden but it is certainly a cost and it should be considered.

Mr. CHABOT. Thank you, very much.

Mr. Chairman, I know the light is ready to turn red here. My follow-up question was just going to be with the other witnesses to see if they wanted to comment on the legislation that we've considered here today, but I'm sure the other Members of the panel will get into that so I'll refrain from asking that at this time.

Mr. CANNON. The gentleman yields back. The gentleman from New York, Mr. Nadler, is recognized for 5 minutes.

Mr. NADLER. Thank you.

Thank you. Let me start by just asking the other witnesses if they'll comment on the questions of the gentleman from Ohio. I would have a similar question on the impact of this legislation. Mr. Dempsey first.

Mr. DEMPSEY. Congressman, if I could. As the Chairman said, of course, the Budget Office has looked at this and concluded that it will not have a significant monetary impact. But I think more importantly than that, these are issues that have to be addressed anyhow in the design of the system. The privacy impact assessment, whether it's on the regulatory side or on the procurement side, you have to—program managers better be addressing what information are they collecting, why are they collecting it, how long are they keeping it for, who's going to have access to it, how the security of it will be protected, how they will ensure the accuracy of the information—after all the system is not going to be worth anything and we're going to just be wasting money if the information is inaccurate—how do citizens correct information in the system, and what sort of oversight and audit mechanism is there?

So those are issues that any good program manager should be addressing strictly from an efficiency standpoint. Again, this is one of the areas where the privacy interest and the Governmental mission are not at odds with each other. You have to walk through the information issues.

I think a better term than privacy is fair information practices. How are we using information? That's one of the things that the PIA process helps you do. And at the end of the day if you don't do that you're going to end up with either an embarrassment or a system that doesn't work or citizen disrespect for the system, in which case perhaps citizens will start entering faulty data, et cetera.

So in order to create trust and in order to create an efficient system to serve the Government mission, whenever it is, you have to address these questions.

That's why I say that I don't really see this at all as imposing a cost. I see it really as helping the efficiency of the Government.

Mr. NADLER. It imposes a cost, in other words, only if the Government agencies weren't going to do what they should be doing?

Mr. DEMPSEY. That's correct.

Mr. NADLER. Does anyone else have a brief comment to make, because I have one other question?

Ms. KATZEN. I would just add one thing to that, sir, and that is, as Mr. Dempsey mentioned earlier, there is already in the law and OMB has issued guidance and the agencies are learning how to do PIAs for not only information technology programs, which is what the CAPPS II and the US-VISIT programs are. They are not regulations, they are programs.

But also the E-Government Act applies whenever there is an information collection, paperwork, that calls for personally identifiable information.

Now, often those paperwork exercises are the product of rules, regulations. And I think it is well taken that it should be clear that the E-Government Act applies in those circumstances.

But I would support what Mr. Dempsey said—make sure they're the two same regimes and not different regimes for the same process.

Mr. NADLER. Thank you.

Ms. Kelly, let me ask you the following. Much of the debate over privacy is centered about the accumulation of information about individuals by Government agencies. But this Committee has been advised on numerous occasions that information gathered by contractors or other third parties is sometimes used or reviewed by those third parties and never actually retained by the Government agency. What steps are Federal agencies—have Federal agencies taken to ensure the information gathered and held by third party contracts for the Federal Government is protected?

And to the extent that some of these data functions are being contracted out overseas what steps are Federal agencies taking to ensure that once the data is outside the U.S. it is not missed used or mishandled abroad?

Ms. O'CONNOR KELLY. Thank you, very much, Mr. Nadler.

I think that the sharing of personal information between the public and the private sector is likely one of the most compelling privacy issues confronted by my department and by most Federal agencies in trying to leverage the best of technology and the most efficient and cost-effective processes to achieve their departmental mission but while also protecting the personal information that is used in those programs or missions.

In my experience at the Department of Homeland Security, we very routinely cover contractors who are providing services to the Department by the Privacy Act expressly in Privacy Act systems of records notices which bind the activities and the behavior of the contractor to be subject to the Privacy Act of 1974 equally as if those activities were performed by a Federal Government employee.

But your point is still extraordinary well taken that in instances that a private sector company is not acting as a contractor but is simply a partner or somehow a regulated entity the rules are less clear. And my office is also working diligently with a number of industry groups to develop responsible rules for that kind of information sharing across the public and private sector divide.

I think some of the points that Ranking Member Watt made earlier about the incidents of information sharing in the past are extraordinarily important and illustrative that we need those kind of rules in place on a voluntary basis in the private sector as well as good instruction in the public sector on how to handle private sector information.

Mr. NADLER. I see the red light so I won't follow up. Thank you.

Mr. CANNON. The gentleman yields back.

Mr. Coble, the gentleman from North Carolina, is recognized for 5 minutes.

Mr. COBLE. Thank you, Mr. Chairman. And Chairman Cannon said earlier, we appreciate you all being with us, I say to each of the four witnesses.

Mr. Chairman, I've got to depart for a meeting that started at four o'clock, but prior to my departure I wanted to put a question to Ms. O'Connor Kelly regarding last fall's disclosure, Ms. O'Connor Kelly, that JetBlue provided travel records I think in excess of one million of its passengers to a defense contractor presumably in violation of its own policies.

I recall there were several press releases or reports shortly after that was revealed that indicated that you were commencing an investigation into matter. I'm curious to know the current status of your investigation.

Ms. O'CONNOR KELLY. Thank you, very much, Mr. Coble.

Again, a very high profile and high priority for my office is the investigation of any misuse of individual data by any employee of the Department of Homeland Security that would violate the Privacy Act. And certainly the case that you refer to is probably one of the more high-profile cases in the last 12 months. We certainly did announce that we were looking into particularly any activities by Department of Homeland Security employees. We are still in the process of accumulating many, many pages of documents that we are reviewing in my office to ascertain any wrongdoing by any employee.

I think though the case illustrates a larger point which is in the days and weeks after September 11th, many companies voluntarily came forward in the spirit of trying to help Federal Government agencies and we need to have clearer rules in place where companies who want to help the homeland security mission know how to do that effectively and with respect for their customers' information and with respect for the privacy policies that are in place at the time that data is collected.

Mr. COBLE. And I also presume or hopefully that their purpose in doing so was well-intentioned. Is that your reading?

Ms. O'CONNOR KELLY. That's very much my understanding, yes, sir.

Mr. COBLE. I thank you and I yield back, Mr. Chairman.

Mr. CANNON. I thank the gentleman. I apologize for causing him to be late by going out of order earlier.

Mr. COBLE. I will hold you harmless.

Mr. CANNON. Thank you, my friend.

The gentleman from Massachusetts, Mr. Delahunt, is recognized for 5 minutes.

Mr. DELAHUNT. Thank you, Mr. Chairman. And Professor Katzen and Mr. Dempsey, to follow up on your reference to how the—this concept, this privacy information office should be expanded, I've had discussions with the gentleman to my right here, although he's usually to my left but today he's to my right, Mr. Nadler. He and I intend to file, and we will be looking for co-sponsors, legislation to insert this—insert this particular initiative into the Department of Justice. So we'll be looking to you for guidance, as well as—as well as you, Ms. Kelly.

Having said that, my concern is about the enforcement mechanism. I think it was the GAO study last year that indicated that

compliance with the Privacy Act by various Federal agencies is—I think the word was uneven. And there—in the memo prepared by the Chairman to Members of the Committee, there's a sentence in there, and let me read it to you. And then I would pose the question and ask comments—ask if you can provide information to the Committee.

An agency that releases such information in violation of the Privacy Act may be sued for damages sustained by an individual as a result of such violation under certain circumstances.

Presumably the—it's the Federal Tort Claims Act that would be implicated? Or is there a different piece of legislation that allows a suit? Professor Dempsey?

Mr. DEMPSEY. I'm not a professor but I think I can answer the question.

It's actually in the Privacy Act itself, where there is a damages provision.

Mr. DELAHUNT. Are there caps on the damages?

Mr. DEMPSEY. No, I don't think there are. There's a liquidated damages provision and then there's also a whatever damages you can prove.

Mr. DELAHUNT. So this outside the Federal Tort Claims Act then?

Mr. DEMPSEY. Yes, it's a separate statutory scheme, yes, sir.

Mr. DELAHUNT. In terms of the enforcement mechanism?

Mr. DEMPSEY. Yes.

Mr. DELAHUNT. Do we have data available to us in terms of the number of suits that have been brought?

Mr. DEMPSEY. Well, one of the issues, actually an issue that's now before the Supreme Court—and it's one we should all watch carefully—is the question of the statutory or liquidated damages provision of that law. In many cases, of course, it may be difficult to prove specific monetary losses, although in the case of a victim of identity theft that could be significant. An awful lot of people sue under the liquidated damages provision where there is a——

Mr. DELAHUNT. You said an awful lot. Do you have any empirical information that you can provide?

Mr. DEMPSEY. Not with me sir, but we could certainly try to find some of that and get——

Mr. DELAHUNT. I really think that's important because we can have a policy but if we have, within the provision allowing for lawsuits by individuals against the Government, impediments that are burdensome then I don't see the necessary deterrence, if you will, to Federal agencies to not comply, if you will.

Mr. DEMPSEY. Well and I—we will definitely look at——

Mr. DELAHUNT. Or incentive. Let me rephrase it, incentive to comply with the Privacy Act.

Mr. DEMPSEY. Congressman, we're happy to look that up.

Mr. DELAHUNT. And if there are settlements, too, I'd like to have that information.

Mr. DEMPSEY. And I think you're also on the right track here generally, which is that you can have an office like the privacy officer, and that's important, but you need to look at the question of what are the laws that he or she is enforcing. And if those laws themselves don't have any teeth to them, then that person is only

as good as their internal persuasive powers are and they're going to win some and lose some.

Mr. DELAHUNT. Well, I'm sure Ms. Kelly's persuasive powers are substantial, but I'd like to have some teeth.

Mr. DEMPSEY. You need some teeth.

Mr. DELAHUNT. In terms of the—again, in terms of creating incentive for compliance because, you know, we can have oversight hearings and we can be people of—we can have all the good intentions in the world. But if we do not have a deterrence, if you will, then I think we will continue to find that compliance will be, as the GAO study indicated, uneven. And that's a real danger.

Anyone else went to comment?

Mr. GILMORE. Mr. Delahunt, let me add one thing. I know the emphasis of the question is on not getting information. There are going to be a large number of programs and Governmental functions that are, by their very nature, going to accumulate some information from people. And then I think, at that point, the real focus needs to be what rules, what technologies, what regulations are applied in order to—how to control that information. Who gets it? Where is it stored? How long is it stored? Who can get it and who can't? What can you do with it?

These are the ultimate issues that are going to provide the security to the people of the United States as we go forward.

For example, there are—Mr. Nadler, Congressman Nadler asked a question about how the Department could influence some of these matters. And I think they're doing it by issuing contracts that place important privacy considerations within them and requirements that private contractors address those issues and actually come forward with their way of dealing with it so that it can be assessed by the Privacy Officer and by the Department.

You are, in effect, beginning to set down the structures and institutional checks and balance necessary that will give you the opportunity for oversight.

Mr. DELAHUNT. Thank you.

Mr. CANNON. The gentleman's time has expired.

Let me suggest to the gentleman from Massachusetts and also the gentleman from New York that I believe we have a provision in this so far unreported DOJ reauthorization bill that we could create the privacy officer for the Department of Justice. So you may want to take a look at that bill and see how that would fit in.

Without objection, Members may submit questions to the witnesses, written questions, and we'll try and include the answers to those in the record, if there are any of those.

And now Mr. Watt, the gentlemen from North Carolina is recognized for 5 minutes.

Mr. WATT. Thank you, Mr. Chairman. I want to pick up on a couple of things that have come out in the testimony, if I have time. The most important one is kind of a segue from your last comment, Mr. Chairman, and from Professor Katzen and Mr. Dempsey's suggestion that we really need to have privacy officers in all 20 departments, however many departments there are.

I may be expecting too much of Ms. Kelly to ask her to comment on that because she's probably going to have the feeling that she would be meddling in other people's business. But I would, if she

cares to comment on it, like to hear from her on whether she thinks that's a good idea. I would certainly like to hear from Governor Gilmore on whether he thinks it's a good idea.

And I guess the subtext for that is is there really enough expertise in our agencies now to do effective privacy impact analyses without a privacy officer? And secondarily, is there enough focus on it, on the importance of it, without having somebody who has direct responsibility for it?

So with those—with that kind of backdrop let me—I'll give Ms. Kelly an opportunity to kind of frame how she might want to meddle in this while we listen to Governor Gilmore.

Mr. GILMORE. Congressman Watt, I guess that the two elements I was thinking about as you asked your question is number one, what is—what are you trying to do? And I think that there's going to be a big debate here as time goes on as we apply security measures about how that impinges on the overall freedoms of the American people. Not just privacy. Privacy is only really a single element. And I know the Subcommittee is focused on it because of the Privacy Act and the underlying House—H.R. 338. But it's going to be a big issue.

But I guess I would want to reflect upon whether or not you want to put 28 privacy officers into all these different departments. It certainly would require an awful lot of staff. It would require an awful lot of slowing up, potentially.

And mainly, I wonder about one privacy officer in one department making a rule on a particular concept and then another privacy officer somewhere else making the same ruling or a different ruling on the same concept. And after a while the Government becomes so snarled up about what's privacy and what isn't that you may really slow things up in a way that could be detrimental.

I'd think about that. You might want to just consolidate all of this under Nuala O'Connor Kelly, give her about 5,000 employees or redeploy them, if you will——

Mr. WATT. Not only now you've got her going to meddling, you've got her to empire building.

Mr. GILMORE. Empire building. But I would redeploy.

Mr. WATT. You've laid a good framework for whatever comment she might want to make.

Mr. GILMORE. I guess those are my initial thoughts.

Mr. WATT. Ms. Kelly?

Ms. O'CONNOR KELLY. Well, I have to say that this entire panel is in violent agreement that we are all very happy with the work that's been done and that there's much more to be done, both at our agency and at other agencies. So you're right, Congressman Watt, that I try not to be meddlesome, although I'm sure that I've been accused of that in my personal life and elsewhere.

But I should note that the OMB guidance under section 208 of the E-Government Act impliedly requires all agencies to have a senior privacy official. And you echo that language in the proposed Federal Agency Protection of Privacy Act, as it's called now.

Mr. WATT. Is there enough expertise on this issue, though, in most agencies, in your opinion, without somebody whose sole responsibility is that?

Ms. O'CONNOR KELLY. There's a surprising amount of expertise in the agencies that have a historic mission that affects personal information. I think it's no accident that you see tremendously well formed privacy programs at agencies like the Internal Revenue Service and the United States Postal Service. I know both of those privacy officers in those programs quite well. Because certainly incidents have happened in the past where people were concerned about those agencies' work but also because such a crucial lifeblood of their mission involves personal information.

I certainly would say that we need to look at the hierarchy of agency missions and of the language of the proposed bill as well in that light, that we certainly may not need PIAs for rules that have absolutely no impact on human beings at all but simply deal with statistics or other intangible objects. But certainly agencies and programs that impact personal information should be, I think, our first line of attack.

Mr. WATT. Go-ahead.

Ms. KATZEN. If I may, I'm not in the Government right now but my experience is that the amount of expertise in the field of privacy has been increasing exponentially, and that we have a cadre of people who understand the concept and know how the Federal Government works and that there would be a good pool to feed this process.

But the solution is to have a statutory office in OMB, the Chief Counselor For privacy, so you would not have the kinds of disagreements among agencies that Governor Gilmore was suggesting.

Mr. WATT. So you're not saying you might not need 20 of them, you might need one super privacy czar, in OMB?

Ms. KATZEN. Exactly. If you had that then you could have a handful of agencies, five or six agencies max, where, as Ms. Kelly has indicated, we have the expertise because for years they have been dealing with personally sensitive information, either financial or medical records, SSA, those kinds of areas, with it topped by an OMB official would be, I think, very sensible.

Mr. DEMPSEY. Congressman Watt, just two quick—two or three quick points.

First of all, the Center for Democracy and Technology, recognizing this question about expertise, has been conducting a series of workshops—we held two last year, we held one in January, we're holding a second one on March 31—for Government officials to help actually walk them through the implementation of the E-Government Act, including the preparation of privacy impact assessments and some of the other provisions there. We've had roughly 150 agency officials at each one of those so far, working with OMB.

Now, I'll say that OMB has not been fully fulfilling, I think, it's mission here. They were late in issuing the guidance on preparation of privacy impact assessments. They clearly have a role to do that. They were late in doing that.

And they're now unfortunately encouraging agencies to withhold the privacy impact assessments that they have done until after the budget process is completed. And really, the whole purpose of the privacy impact assessment is to do it, get it out there for comment so that both this Congress and members of the public can take a look at it and comment upon it before something is set in stone.

I think the recommendation of Ms. Katzen is 100 percent correct, that one way perhaps to strike the right balance here is to have that designated chief privacy counselor in OMB, preferably with some statutory basis, and then to go agency by agency where it's particularly necessary, with the Department of Justice, with the Social Security Administration. We have two very, very good non-statutory privacy officers at the Postal Service and at the IRS, both of whom are excellent but have no real statutory basis. And those are agencies that clearly need them.

Mr. WATT. Thank you, Mr. Chairman. You've been very generous.

Mr. CANNON. We appreciate it. Thank you, Mr. Watt. The gentleman yields back.

And we thank the panel for your comment. I do have a couple of comments but first of all, without objection, Members will have—be allowed 7 days to submit questions [1] for the members of the panel. Hearing no objection, so ordered.

Let me just point out that the testimony today was appropriate and interesting and remarkably coherent. And I think we have our work cut out for us here. May I just say, in the first place, we intend to oversee this process rigorously. And secondly, we will take the comments and suggestions very much into consideration between now and the time that we mark up this bill at full Subcommittee and appreciate that.

I believe at this point that there is good reason to have more statutory—more privacy officers with statutory authority. I think that's worked very well. I said earlier that I thought that Ms. O'Connor Kelly's work was historic and, in fact, I think it is groundbreaking and it's the foundation for what we do.

I might just add my own comments. I think the Administration has done a remarkably good job in this regard. And maybe it's a little different. Somebody called it—said we ought to have a czar, a privacy czar at OMB. I forget who actually used that term.

But my sense is that having done what we've done at DHS, and which Ms. O'Connor Kelly has really led on, gives us a much better sense of what can be done and frankly and particularly the importance of statutory authority, which I think Mr. Dempsey you talked about with particularity.

I think that that has a tendency to grow the ideas. And I view that if we get a privacy czar at OMB, I wouldn't think of him as a czar so much as a best practices kind of person who is watching what happens. Because I don't think you can force privacy down. I think you need agencies to get the gospel, which is that if you—and I think you said this with great clarity, Mr. Dempsey. If you consider these in the design of the program with regulation, you end up with a much lower cost overall and a much better outcome.

My experience with OMB, and I don't mean to disagree with you on this, Ms. Katzen, but it's always very bitter. It's just difficult when you're pounding on these guys who have great authority.

---

[1] Post-hearing questions were submitted by the Honorable Chris Cannon, Chairman of the Subcommittee, to Ms. Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Department of Homeland Security. No response had been received by the Subcommittee at the time this hearing was printed. A copy of the questions submitted by Mr. Cannon can be found in the Appendix.

And I don't think this is an issue that resolves itself well by a young person who comes in the Government and serves in OMB where he is given a robe of authority that transcends anything he could imagine or she could imagine in advance of that, and now is going to tell people who have actually got experience in an and agency and in the problems and the programs of that agency, how they're going to do business. I think it works much better if it goes the other way.

But we are going to deal with that issue I can assure you, and I suspect we're going to see several more privacy officers because I think this has worked out well.

So I thank the panel and Members for coming today. With that, we will stand adjourned.

[Whereupon, at 4:35 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

February 26, 2004

Ms. Nuala O'Connor Kelly
Chief Privacy Officer
United States Department of Homeland Security
Washington, DC 20528

Dear Ms. Kelly:

Thank you for appearing before the Subcommittee on Commercial and Administrative Law at the legislative oversight hearing on "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security" on February 10, 2004. Your testimony, and the efforts you made to present it, are deeply appreciated and will help guide us in whatever action we take on this matter.

Pursuant to the unanimous consent request agreed upon at the hearing, Subcommittee Members were given the opportunity to submit written questions to the witnesses. These questions are annexed. Your response will help inform subsequent legislative action on this important topic.

Please submit your written response to these questions by 5:00 p.m. on Monday, March 15, 2004, to: Susan Jensen, Counsel, Subcommittee on Commercial and Administrative Law, B353 Rayburn House Office Building, Washington, DC 20515. Your responses may also be submitted by e-mail to: susan.jensen@mail.house.gov

In addition, we have enclosed for your review a copy of the official transcript of this hearing. The transcript is substantially a verbatim account of remarks actually made during the hearing. Accordingly, please only make corrections addressing technical, grammatical, or typographical errors. No substantive changes are permitted. Please return any corrections you have to: Susan Jensen, Subcommittee on Commercial and Administrative Law, B353 Rayburn House Office Building, Washington, DC 20515 by Monday, March 15, 2004.

If you have any questions regarding the enclosed questions or transcript, please feel free to contact Ms. Jensen at (202) 225-2825.

Thank you for your continued assistance.

Sincerely,

CHRIS CANNON
Chairman
Subcommittee on Commercial and Administrative Law

Enclosures
CC/sj

c: The Honorable Mel Watt

1. In what ways have you fulfilled your statutory duty to assure that "the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information"?

2. In what ways have you fulfilled your statutory duty to assure that "personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974"?

3. Does the statute that created your position at the Department of Homeland Security (DHS) provide sufficient guidance and direction?

4. Are there any legislative tools that would assist you in better carrying out your responsibilities?

5. How do you deal with a situation where management rejects a recommendation that you have made?

6. How do you respond to skeptics who question your independence from management?

7. Is your office sufficiently staffed and funded in order for you to execute your statutory responsibilities?

8. To what extent do you coordinate with privacy officers in other agencies? Are there shared problems/solutions?

9. In what ways has the DHS Privacy Office influenced the development of the Department's CAPPS II program reported in the media?

10. How do you respond to the concern that CAPPS II will turn airports into all-purpose checkpoints?

11. The Electronic Privacy Information Center claims that the collection of personal data in the name of homeland security is "part of an ambitious but misdirected effort to mine all kinds of data." What is your response to this charge?

12. What are your views about H.R. 338, the "Federal Agency Protection of Privacy Act"?

13. When can we expect to receive your annual report to Congress activities of the Department that affect privacy? This report, as you know, must identify any complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.

14. Would you recommend that other federal agencies have statutorily mandated privacy officer positions?

15. Some in the law enforcement community wonder if protection of privacy initiatives will undercut their terrorism and crime detection efforts. How do you respond?